

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005年1月27日 (27.01.2005)

PCT

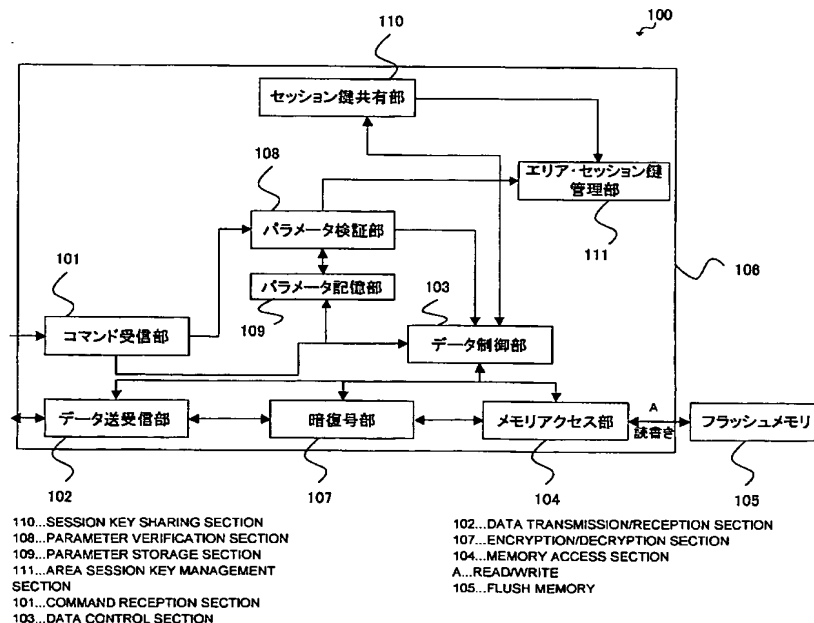
(10) 国際公開番号
WO 2005/008502 A1

- (51) 国際特許分類⁷: G06F 12/14, G06K 17/00
- (21) 国際出願番号: PCT/JP2004/010432
- (22) 国際出願日: 2004年7月15日 (15.07.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-275672 2003年7月16日 (16.07.2003) JP
特願2004-197453 2004年7月2日 (02.07.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真1006番地 Osaka (JP).
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 高木 佳彦 (TAKAGI, Yoshihiko). 菊地 隆文 (KIKUCHI, Takafumi).
- (74) 代理人: 鷺田 公一 (WASHIDA, Kimihito); 〒2060034 東京都多摩市鶴牧1丁目24-1 新都市センタービル5階 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: ACCESS METHOD

(54) 発明の名称: アクセス方法



(57) Abstract: A command specifying an access region from a terminal is separated from a command performing access and the argument of the command performing access contains terminal verification data when transmitted. Thus, it is possible to verify that the terminal application which has issued the command specifying the access region, the terminal application which has issued the command performing access, and the terminal application holding the authentication key are the same.

(57) 要約: 端末からアクセス領域を指定するコマンドと、アクセスを行うコマンドを分離し、アクセスを行うコマンドの引数に端末の検証データを含めて送信することで、アクセス領域を指定するコマンドを発行した端末アプリケーションとアクセスを行うコマンドを発行した端末アプリケーションと、検証用鍵を保有する端末アプリケーションが同一であることが検証可能となる。

BEST AVAILABLE COPY



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

明 細 書

アクセス方法

5 技術分野

本発明は、P Cや携帯電話などの端末に挿入して使用されるメモリカード、並びにメモリカードに対するアクセス方法に関する。

背景技術

- 10 従来、メモリカードは端末に挿入され、端末がデータを格納するためのものである。以下に、従来のメモリカードの一例をあげる（例えば、特願2003-91704号公報）。

- カードは、端末から各種コマンドを受け付け、またコマンドに対するレスポンスを返すコマンド用端子（CMDライン）と、データの入力を受け付け、またデータの出力を行うデータ用端子（DATライン）を持つ。
- 15

- 図1に示した従来のメモリカードの例では、端子4602がCMDラインとなっており、端子4607、4608、4609がDATラインであり、それぞれDAT0、DAT1、DAT2となっている。また端子C2-01はデータ入出力用とカード検出用（CD）を兼ねたCD/DAT3となっている。DAT0～DAT3については、DAT0のみを使うモードと、DAT0～3を同時に利用しDAT0のみを使う場合の4倍の転送速度を実現するモードが存在する。
- 20

次に、図2を用いて、従来カードのカード内モジュール構成について説明する。

- 25 カード内モジュールは、CMDライン4602に接続された、コマンド受信及びレスポンス送信を行う処理命令受信手段4701と、DATライン4607、4608、4609、C2-01に接続された、データ送受信を行うデー

タ送受信手段4702と、記憶領域4704と、受信したコマンドに応じて記憶領域4704へのデータの読み書きを行う記憶領域アクセス手段4703からなる。

- 次に、従来のメモリカードにおける、データ読み出し時の処理動作について
- 5 説明する。ここではデータの出力はDAT0端子4607のみを利用するモードに設定されているものとするが、DAT1端子4608、DAT2端子4609、DAT3端子4610を併用するモードであってもよい。

- まず、端末はカードのCMDライン4602にデータ読み出しコマンドを送信する。この読み出しコマンドは図7で示されるフォーマットとなっており、
- 10 6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。データ読み出しコマンドにおけるコマンド引数は、読み出し開始アドレスを格納する。

端末からコマンドを受信した処理命令受信手段4701は、コマンドコード401を参照して、データ読み出しコマンドであることを認識する。

- 15 次に、処理命令受信手段4701は、コマンド引数402を参照して、指定されたアドレスが正しいものであるか、つまりカードが対応している範囲に指定されたアドレスが収まっているかを調べ、アドレスが正しくなければレスポンスとしてエラーである旨のレスポンスコードを返す。アドレスが正しければ正常である旨のレスポンスコードを返す。

- 20 処理命令受信手段4701は、レスポンスを端末に返送した後、記憶領域アクセス手段4703に対し、指定されたアドレスとともに、読み出し要求を行う。

記憶領域アクセス手段4703は、記憶領域4704の指定アドレスからデータを読み出し、データ送受信手段4702に送信する。

- 25 データ送受信手段4702は、DAT0ライン4607を通じて、端末に読み出しデータの出力を行う。

このようなメモリカードでは、端末からアドレスを指定して自由にカードの

読み書きが可能である。

上記のようなメモリカードにおいて、フラッシュメモリの特定領域をセキュリティ保護領域としてアクセス制限をかけ、アクセスが許可された特定の端末からのみアクセス可能としたい場合に、上記文献で示されたカードでは、I C
5 カードコマンドを用いて柔軟な認証を行うことが可能である。しかし、I Cカードの標準的なコマンドフォーマットであるAPDU (Application protocol data unit) では、256バイトのデータ送受信しか行えないことと、半二重プロトコルのために、ホストからのコマンド送信の度にレスポンス受信が必要であるという理由から、高速なデータ転送が困難である。そこで、I Cカードコマンド
10 マンドを用いて、セキュリティポリシーに柔軟にあわせた方式にて認証処理を行った後でメモリカードコマンドを用いてデータ転送を行う方式が考えられるが、I Cカードコマンドの発行者とメモリカードコマンドを発行したホスト上のアプリケーションが同一であることを確認することが困難である。

そこで、I Cカードコマンドを用いた認証処理の過程で生成した情報を、I
15 Cカードコマンドとメモリカードコマンドの発行者の同一性を検証するための検証データとしてメモリカードコマンドに含める場合、コマンド引数にアクセス領域指定情報 (アクセスするアドレスなど) と認証用の検証データを含めることになるが、データ読み出しコマンドのコマンド引数402のサイズは上述の通り、32ビットの固定であるので、セキュリティを向上させるため認証
20 用の検証データのサイズを大きくすると、アクセス領域指定情報の長さが短くなりアクセス可能な領域が制限されてしまう。一方、検証データのサイズを小さくすれば、セキュリティ強度が下がってしまう。

この課題を解決するために、従来のデータ読み出しコマンドのフォーマットを変更すると、従来のメモリカードにアクセスができなくなってしまうおそれ
25 がある。

また、従来のデータ読み出しコマンドと、セキュリティ保護領域を備えたメモリカードへのデータ読み出しコマンドとを別個のものとして併存させると

すると、端末側でメモリカードの種類によってコマンドを切り換える必要が発生し、メモリカードへのアクセスが複雑となり、端末にとっては利用しづらいものとなる。そのため、検証データを送信するためのコマンドとデータの読み出しまたは書き込みを行うためのメモリカードコマンドをそれぞれ定義し、2
5 つのコマンドを組み合わせ、セキュリティ保護領域へのアクセスを行う必要があるが、2つのコマンドの間でコマンド発行者の同一性を確認することができない。

発明の開示

10 本発明は、これらの問題点を解決するものであり、メモリカード内でアクセス制限がされていない領域にアクセスする場合は、上述のデータ読み出しコマンドに代表されるメモリカードコマンドを用い、アクセス制限がされているセキュリティ保護領域に関しては、まずアクセス領域を指定するメモリカードコマンドによってアクセス領域指定情報をメモリカードに送付した後に、ホスト
15 とメモリカード間でICカードコマンドを用いた柔軟な認証処理を用いて共有した、または、予め共有している鍵情報と、上記アクセス領域指定情報を用いて生成した認証用の検証データを含ませた、セキュリティ保護領域の読み出しまたは書き込み用メモリカードコマンドをメモリカードに送付して、セキュリティ保護領域へのデータの書き込み、セキュリティ保護領域からのデータを
20 読み出しする、という2段階のコマンド構成にすることで、メモリカードコマンドのフォーマットの変更を必要とせず、また少ないコマンド引数でもセキュリティを低下させることなく、セキュリティ保護領域へのアクセスを可能にするアクセス方法を提供することを目的とする。

本発明の一形態によれば、アクセス方法は、機器からメモリデバイスに対する
25 アクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリ

デバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明の他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、検証用鍵を共有化するステップと、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記メモリデバイスとで、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス

領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

る。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命

- 令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて
- 5 成功した場合、前記処理命令を実行するステップと、を有する。

- 本発明のさらに他の形態によれば、メモリデバイスは、機器から読み書きされるメモリデバイスであって、アクセスする領域を指定する指定情報を受信するとともに、前記指定情報に基づく検証情報と読み出し又は書き込み命令を併せて受信する処理命令受信手段と、前記指定情報を、前記検証情報を用いて検証
- 10 処理を行う指定情報検証手段と、データを格納する記憶領域と、前記検証処理が成功した場合に、前記処理命令に応じて、前記記憶領域の前記指定領域に対する読み出し又は書き込みを行う記憶領域アクセス手段と、前記記憶領域アクセス手段が読み出したデータを前記機器に送信するデータ送信手段と、前記機器から書き込みデータを受信するデータ受信手段と、を備える。

- 15 本発明のさらに他の形態によれば、情報機器は、メモリデバイスを読み書きする情報機器であって、読み出し又は書き込みする領域を決定し、前記領域を指定する指定情報を決定する指定情報決定手段と、前記指定情報から前記検証情報の生成処理を行う検証情報生成手段と、前記指定情報の送信と、前記検証情報と読み出し又は書き込みの処理命令とを併せて送信する処理命令送信手
- 20 段と、前記処理命令が書き込みの場合は、前記メモリデバイスにデータを送信するデータ送信手段と、前記処理命令が読み出しの場合は、前記メモリデバイスからデータを受信するデータ受信手段と、前記メモリデバイスに送信するデータを記憶し、または、前記メモリデバイスから受信したデータを記憶するデータ記憶手段と、を備える。

- 25 本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処

- 理命令と、前記指定情報に関する検証情報を検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと検証用鍵とを用いて検証するステップと、前記検証に成功した場合、前記処理命令を実行するステップと、を有する。

- 本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器は、第一の処理系コマンドを用いて前記メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて前記アクセス可能領域に対応した検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合は、前記処理命令を実行するステップと、を有する。

- 本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性かつ大容量の第2領域と、前記機器からアクセスすることが可能なかつ大容量の第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて、前記アクセス可能領域に対応した検証用鍵を共有化するス

- テップと、第二の処理系コマンドを用いて、前記第 2 領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

10 図面の簡単な説明

- 図 1 は、従来のメモリカードの端子構成を示す図、
図 2 は、従来のカード内モジュール構成を示す図、
図 3 は、本発明の実施の形態 1 に係るメモリカードの内部モジュール構成を示す図、
15 図 4 は、本発明の実施の形態 1 に係るカードの端子構成を示す図、
図 5 は、本発明の実施の形態 1 に係る端末の内部構成を示す図、
図 6 は、本発明の実施の形態 1 に係るカードと端末の間で行われる処理の概要を示す図、
図 7 は、本発明の実施の形態 1 に係る A P D U の送受信方法のシーケンスを示す図、
20 図 8 は、本発明の実施の形態 1 に係るレスポンス A P D U の送信処理のシーケンスを示す図、
図 9 は、本発明の実施の形態 1 に係るメモリカードのコマンドフォーマットを示す図、
25 図 10 は、本発明の実施の形態 1 に係るフラッシュメモリの内部構成を示す図、
図 11 は、本発明の実施の形態 1 に係るセキュリティ保護領域の内部構成を

示す図、

図 1 2 は、本発明の実施の形態 1 に係るセキュリティ保護領域内の各アプリケーション用領域の内部構成を示す図、

図 1 3 は、本発明の実施の形態 1 に係るセッション鍵共有及びアクセス可能
5 領域共有手順を示す図、

図 1 4 は、本発明の実施の形態 1 に係る図 1 3 のステップ 9 0 3 における処理の詳細を説明するためのフローチャート、

図 1 5 は、本発明の実施の形態 1 に係る図 1 3 のステップ 9 0 5 における処理の詳細を説明するためのフローチャート、

10 図 1 6 は、本発明の実施の形態 1 に係る図 1 1 のステップ 9 0 7 における処理の詳細を説明するためのフローチャート、

図 1 7 は、本発明の実施の形態 1 に係る端末からセキュリティ保護領域を読み出すためのコマンドシーケンスを示す図、

図 1 8 は、本発明の実施の形態 1 に係る A P D U 送信コマンドの引数フォーマットを示す図、
15

図 1 9 は、本発明の実施の形態 1 に係る A P D U 受信コマンドの引数フォーマットを示す図、

図 2 0 は、本発明の実施の形態 1 に係る A P D U 送信コマンドの入力データ及び A P D U 受信コマンドの出力データのフォーマットを示す図、

20 図 2 1 は、本発明の実施の形態 1 に係るアクセス領域指定コマンドの入力データフォーマットを示す図、

図 2 2 は、本発明の実施の形態 1 に係るアクセス領域指定情報を示す図、

図 2 3 は、本発明の実施の形態 1 に係る端末の正当性検証を行うための検証データの端末による生成方法を示す図、

25 図 2 4 は、本発明の実施の形態 1 に係る端末の正当性検証を行うための検証データのカードによる生成方法を示す図、

図 2 5 は、本発明の実施の形態 1 に係る端末からセキュリティ保護領域に書

き込むためのコマンドシーケンスを示す図、

図 2 6 は、本発明の実施の形態 2 に係るメモリカードの内部モジュール構成を示す図、

図 2 7 は、本発明の実施の形態 2 に係る端末の内部構成を示す図、

- 5 図 2 8 は、本発明の実施の形態 2 に係る端末からカードのセキュリティ保護領域に対してアクセスを行う際の処理を示すフローチャート、

図 2 9 は、本発明の実施の形態 2 に係る領域指定命令のデータ部の一例を示す図、

- 図 3 0 は、本発明の実施の形態 2 に係る図 2 9 のアクセス領域指定情報のフ
10 ォーマットを示す図、

図 3 1 は、本発明の実施の形態 2 に係る比較情報の生成方法の一例を示す図、

図 3 2 は、本発明の実施の形態 2 に係る内部に検証用鍵共有手段を備える場合のカード構成を示す図、

- 図 3 3 は、本発明の実施の形態 2 に係る内部に検証用鍵共有手段を備える場
15 合の端末構成を示す図、

図 3 4 は、本発明の実施の形態 2 に係る検証用鍵の共有方法のシーケンスを示す図、

図 3 5 は、本発明の実施の形態 2 に係る検証用鍵生成方法を説明するための図、

- 20 図 3 6 は、本発明の実施の形態 2 に係る S H A - 1 演算を用いた比較情報生成方法を示す図、

図 3 7 は、本発明の実施の形態 2 に係る検証情報生成方法を示す図、

図 3 8 は、本発明の実施の形態 2 に係るアクセス命令のフォーマットを示す図、

- 25 図 3 9 は、本発明の実施の形態 2 に係る数情報を利用した検証データ生成処理を示すフローチャート、

図 4 0 は、本発明の実施の形態 2 に係る乱数を利用した比較情報生成方法を

示す図、

図 4 1 は、本発明の実施の形態 2 に係る乱数を利用した検証情報生成方法を示す図、

図 4 2 は、本発明の実施の形態 3 に係るメモリカードの内部モジュール構成
5 を示す図、

図 4 3 は、本発明の実施の形態 3 に係る端末の内部構成を示す図、

図 4 4 は、本発明の実施の形態 3 に係る端末からカード内のセキュリティ保護領域へのアクセス処理の一部を示すフローチャート、

図 4 5 は、本発明の実施の形態 3 に係る図 4 4 に続くアクセス処理の一部を
10 示すフローチャート、

図 4 6 は、本発明の実施の形態 3 に係るアクセス有効テーブルの一例を示す図、

図 4 7 は、本発明の実施の形態 1 に係るアクセス有効テーブルの一例を示す図である。

15

発明を実施するための最良の形態

以下、本発明の実施の形態について、添付図面を参照して詳細に説明する。なお、本発明は、この実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々の形態で実施することができる。

20 (実施の形態 1)

本発明におけるカード内モジュール構成について図 3 を用いて説明する。なお、カード 100 の端子配置は、図 4 に示すが、その端子構成は、図 1 に示したものと各端子に付した符号は異なるが、その構成は同様であるため、説明は省略する。

25 カード内モジュールは、コントローラ 106 とフラッシュメモリ 105 からなる。コントローラ 106 は、CMDラインに接続された、コマンド受信及びレスポンス送信を行うコマンド受信部 101 と、DATラインに接続されたデ

ータ送受信部 102 と、データ送受信部 102 が送受信したデータに対してセッション鍵で暗復号処理を施し、またフラッシュメモリ格納用鍵で暗復号してメモリアクセス部 104 とのデータ受け渡しを行う暗復号部 107 と、フラッシュメモリ 105 へのデータの読み書きを行うメモリアクセス部 104 と、受信したコマンドに応じて、メモリアクセス部 104、セッション鍵共有部 110、及びパラメータ検証部 108、暗復号部 107 に対して処理要求を行うデータ制御部 103 と、端末 200 から受信したセキュリティ保護領域にアクセスするためのパラメータを記憶しておくパラメータ記憶部 109 と、パラメータが正しいことを検証するパラメータ検証部 108 と、端末 200 との間で認証用及び暗復号用のセッション鍵を交換するセッション鍵共有部 110 と、セッション鍵と、セッション鍵と対応付けられたセキュリティ保護領域を記憶しておくエリア・セッション鍵管理部 111 からなる。

次に、本実施の形態 1 における端末 200 の構成について図 5 を用いて説明する。

15 端末 200 は、カード 100 にメモリカードコマンドを送信するコマンド送信部 204 と、カード 100 の DAT ラインにデータを送信するデータ送受信手段 207 と、データ送受信手段 207 が送信するデータを暗号化し、また受信するデータを復号化する暗復号手段 206 と、カード 100 との間でセッション鍵の共有処理を行うセッション鍵共有手段 202 と、セキュリティ保護領域アクセスコマンドによってアクセスする領域を決定し、領域指定情報を生成する、指定情報決定手段 201 と、領域指定情報とセッション鍵から検証データを生成する検証データ生成部 203 と、送信するデータ、または受信したデータを記憶するデータ記憶手段 205 とを備える。

次に、図 3 のカード 100 と図 5 の端末 200 の間で行われる処理の概要について図 6 を用いて説明する。

図 6 において、まず、端末 200 とカード 100 の間では、カード 100 IC カードコマンドを用いた処理として、端末 200 とカード 100 相互間を認

証するための認証処理及びセッション鍵を共有するための鍵共有処理と、端末200からカード100内メモリへのアクセス可能領域の領域番号（図中の領域No. x）を割り当てる領域番号割り当て処理とが実行される（ステップS401）。

- 5 認証処理を行い、相互に正当性が確認された後、鍵共有処理及び領域番号割り当て処理が行われ、その結果として、端末200内とカード100内には、領域No. xにて示されるセキュリティ保護領域へのアクセスを可能にする検証用及び暗号用のセッション鍵が領域番号（領域No. x）と対応付けて保持される。
- 10 次に、端末200とカード100の間では、メモリカードコマンドを用いた処理として、端末200からカード100へのアクセス領域指定コマンド送信処理（ステップS402）及びデータ転送コマンド送信処理（ステップS403）と、カード100から端末200への暗号化データ送信処理（ステップS404）とが実行される。
- 15 アクセス領域指定コマンド送信処理では、アクセスしたいセキュリティ保護領域内の領域を指定するため、領域No. x、ブロックアドレス及びブロック長を設定したデータを含むアクセス領域指定コマンドが端末200からカード100へ送信される。カード100では、受信したアクセス領域指定コマンドから抽出した領域No. xに基づいてセキュリティ保護領域へのアクセス可
20 否検証処理が実行される。

- また、データ転送コマンド送信処理では、端末200において領域No. x、ブロックアドレス及びブロック長と、ステップS401にてカード100との間で共有した検証用鍵を用いて検証データが作成され、この検証データを含むデータ転送（Read）コマンドがカード100に送信される。カード100
25 では、受信したデータ転送（Read）コマンドから端末200との間で共有した検証用鍵の公開鍵を用いて領域No. x、ブロックアドレス及びブロック長を元に検証データを作成していることを確認することで、ステップS402

にて指定されたセキュリティ保護領域へのアクセス可否が検証される。

また、暗号化データ送信処理では、カード100において上記検証処理においてアクセス可となったカードアプリケーションに対応する領域No. xに格納されたデータが、端末200との間で共有した暗号用鍵を用いて暗号化され、

5 この暗号化データが端末200に送信される。

以下の説明では、上記処理概要に処理手順について詳細に説明する。

端末200とセッション鍵共有部110との間で送受信されるコマンド形態は、一般的なICカードで用いられるAPDUフォーマットに従った形とする。つまり、セッション鍵共有部110はICカードアプリケーションの形態

10 をとる。

ここでは、APDUの送受信方法について、図7のシーケンス図を用いて説明する。

まず、端末200からカード100に対するコマンドAPDUの送信処理について説明する。ここで、コマンドAPDUとは、メモリカード側で実行させ

15 たいコマンドをAPDUフォーマット形式で端末200からメモリカード送付するものをいい、具体的にはICカード用コマンドを使用する。

まず、端末200はセッション鍵共有部110に対して送信するコマンドAPDUを作成する。次に、端末200は図2のカード100のCMDライン22に対して、APDU送信コマンドを送信する（ステップS501）。

20 このAPDU送信コマンドは、従来のデータ読み出しコマンドと同様、図7で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

APDU送信コマンドにおけるコマンド引数402は、図18で示すように、DAT0ライン27に入力するデータがコマンドAPDUであることを示す

25 フラグ1401と送信データ数を示す1403とからなる。フラグ1401及び送信データ数1403を合わせて32ビットに満たない場合は未使用フィールド1402が存在する。

図4のDAT0ライン27に入力するデータは512バイト単位となっており、送信データ数1403は、この512バイト単位の入力を何回行うかを示す。

次に、カード100のコマンド受信部101は、端末200から送信された
5 コマンドを受信し（ステップS502）、それがAPDU送信コマンドであることを認識し、CMDライン22を介して端末200にレスポンスを返すとともに（ステップS503）、データ制御部103に対して、APDU送信コマンドを受信したことを通知する（ステップS504）。

次に、端末200はカード100のCMDライン22からAPDU送信コマ
10 ンドに対するレスポンスを受信し（ステップS503）、DAT0ライン27に図20で示すフォーマットでコマンドAPDU1602を入力する（ステップS505）。

図20において、1601で示される長さは後に続くAPDU1602の長さを示している。長さフィールド1601とAPDU1602の合計長にあわ
15 せてコマンド引数の送信データ数1403が設定されている。また、前記合計長は必ずしも512バイトの倍数になるわけではないので、512バイトの倍数になるようにパディング1603を付加する。

次に、カード100内部のデータ送受信部102は、端末200からDAT
0ライン27に入力されたコマンドAPDUを受信するとともに（ステップS
20 505）、データ制御部103にコマンドAPDUを受信したことを通知する（ステップS506）。次に、データ制御部103は、データ送受信部102からコマンドAPDUを読み出し（ステップS507）、セッション鍵共有部110（ICカードアプリケーション）にコマンドAPDUを渡す（ステップS508）

25 次に、セッション鍵共有部110は、コマンドAPDUに記述されたとおりの処理を行い（ステップS509）、処理の結果生じたデータとステータス情報をレスポンスAPDUとしてデータ制御部103に渡す（ステップS51

0)。このステータス情報とは、ISO 7816で定義されたステータスワードであり、正常終了したか、異常終了したかを示す2バイトの値である。

次に、カード100から端末200に対するレスポンスAPDUの送信処理について、図8のシーケンス図を用いて説明する。ここでレスポンスAPDU
5 とは、カード100が実行したコマンドAPDUの処理結果をカード100から端末200へ送信するものをいう。

ここでは、前記のコマンドAPDUの送信方法で示したとおり、セッション鍵共有部110が出力したレスポンスAPDUがデータ制御部103で保持されている状態であるものとする。

10 まず、端末200は、カード100のCMDライン22に対して、APDU受信コマンドを送信する(ステップS601)。このAPDU受信コマンドは、APDU送信コマンドと同様、図9で示される従来のデータ読み出しコマンドと同様のフォーマットとなっており、6ビットのコマンドコード401と32
ビットのコマンド引数402から構成される。

15 APDU受信コマンドにおけるコマンド引数402は、図19で示すように、未使用フィールド1501と送信データ数1502とからなる。送信データ数1502が32ビットに満たない場合は未使用フィールド1501が存在する。

図4のDAT0端子27から出力されるデータは、APDU送信コマンドに
20 おける入力データと同様に512バイト単位となっており、送信データ数1502は512バイト単位で何回出力を行うかを示す。

次に、カード100のコマンド受信部101は、端末200から送信されたコマンドを受信し(ステップS602)、それがAPDU受信コマンドであることを認識し、CMDライン22を介して端末200にレスポンスを返すとともに(ステップS603)、データ制御部103に対して、APDU受信コマ
25 ンドを受信したことを通知する(ステップS604)。

次に、データ制御部103は、データ送受信部102に対して、セッション

鍵共有部 110 から受け取ったレスポンス APDU を渡す（ステップ S605）。

次に、端末 200 は、カード 100 の CMD ライン 22 から APDU 受信コマンドに対するレスポンスを受信し（ステップ S603）、DAT0 ライン 27 を介してデータ送受信部 102 からレスポンス APDU を読み出す（ステップ S606）。読み出されるレスポンス APDU は、図 20 で示すフォーマットで出力される。各フィールドの詳細については、APDU 送信コマンドにおける入力時と同様であるため、説明を省略する。

カード 100 に搭載されるフラッシュメモリ 105 は、図 10 に示すように、少なくとも端末 200 から従来の読み出し用コマンド及び書き込み用コマンドに代表されるメモリカードコマンドでアクセスすることが可能な通常領域（非耐タンパ性のメモリ領域）62 と、前記の従来のコマンドではアクセスすることができないセキュリティ保護領域（耐タンパ性のメモリ領域）61 を持つ。また、カード 100 は、図 10 に示すように、IC カードコマンドでアクセスすることが可能な耐タンパ領域（TRM : tamper resistant module）80 を持つ。

セキュリティ保護領域 61 は、通常、カードアプリケーションからのみアクセス可能な状態であって、端末 200 からの従来の読み出し用コマンド及び書き込み用コマンドに対しては、コマンド受信部 101 によってアクセスは排除される。

本発明におけるメモリカードは内部に複数のカードアプリケーションを搭載することが可能となっており、図 11 に示すように、セキュリティ保護領域 61 は各アプリケーションに対して個別の領域（AP1 用領域 71 ~ AP3 用領域 73）を割り当てることが可能である。

セキュリティ保護領域 61 は、データ制御部 103 が管理する格納用暗号鍵（Ks）で暗号化されている。この暗号鍵は、セキュリティ保護領域 61 全体で 1 つの Ks であってもよいし、各アプリケーション用の AP1 用領域 71 ~

AP 3用領域 7 3 に個別に格納用暗号鍵 $Ks_1 \sim Ks_3$ を用意してもよい。本実施の形態では各アプリケーション AP 1 ~ 3 に格納用暗号鍵 $Ks_1 \sim Ks_3$ を用意する。

- 次に、セキュリティ保護領域 6 1 内の各アプリケーション用の AP 1 用領域
- 5 7 1 ~ AP 3 用領域 7 3 の内部構成について、図 1 2 を用いて説明する。

ここでは、例としてカードアプリケーション AP 1 用領域 7 1 をあげている。AP 1 用領域 7 1 の内部はディレクトリ DIR 1, DIR 2 とファイル FILE 1 ~ FILE 3 を用いた階層構造を用いたデータ管理となっている。

- カードアプリケーション AP 1 は、AP 1 用領域 7 1 内でディレクトリ移動
- 10 を行い、目的のファイルが存在するディレクトリ DIR 1, DIR 2 上でファイル FILE 1 ~ FILE 3 に対する読み書きを行う。

- 例えば、カードアプリケーション AP 1 がファイル FILE 3 にアクセスする場合は、ディレクトリ DIR 1 に移動し、次にディレクトリ DIR 2 に移動した後、ファイル FILE 3 の読み書きを行う。また、各ディレクトリ DIR
- 15 1, DIR 2 において、その下位のディレクトリまたはファイルの作成及び削除が可能である。

次に、カード 1 0 0 内のセッション鍵共有部 1 1 0 と、端末 2 0 0 との間で行われるセッション鍵共有手順について図 1 3 ~ 図 1 6 を用いて説明する。

- カードアプリケーションと端末 2 0 0 はそれぞれ公開鍵暗号で用いられる
- 20 公開鍵と秘密鍵の対を保持し、お互いに相手の公開鍵を保持している。

セッション鍵共有手順におけるコマンド形態は前記で示した APDU を用いる。以降の説明においてはコマンド形態に関する記述を行わず、単にコマンド APDU、レスポンス APDU と表記する。

- まず、端末 2 0 0 は、SELECT コマンド APDU を送信することで、カ
- 25 ードアプリケーション AP 1 の選択を行う (ステップ 9 0 1)。SELECT コマンド APDU とは、以降の IC カード コマンド (コマンド APDU) をカード 1 0 0 内部のどのアプリケーションに送信するかを指定するコマンド A

PDUであり、他のコマンドAPDUと同様にAPDU送信コマンドを用いて送信する。

カード100は、端末200から指定されたカードアプリケーションAP1
の選択が正常に完了すれば正常完了のレスポンスAPDU、完了しなければ異常
5 終了のレスポンスAPDUを返す（ステップ902）。

次に、端末200は、処理903を実行する。この処理903について簡単に説明すると、選択したカードアプリケーションAP1にアクセスすることを可能にするDATA2を生成するための処理である。この処理903の詳細については、図14のフローチャートを参照して説明する。

10 端末200は、乱数Rhの生成を行い（ステップS9031）、乱数Rhと、
端末200がアクセスしたい図12で示したファイルFILE3のファイル
名を結合し、カードアプリケーションAP1が保持する秘密鍵PriSに対応
した公開鍵PubSで暗号化してDATA1を生成し（ステップS9032）、
さらに端末200が保持する秘密鍵PriHに対応した公開鍵PubHを示
15 す識別子Info_PubHとDATA1を結合してDATA2を生成する
（ステップS9033）。

図13に戻り、次に、端末200は、カードアプリケーションとのセッション鍵の共有及び、端末200がアクセス可能な領域情報の共有を行うために、
ステップS9033で生成したDATA2を含んだREQ__AREA__IN
20 FOコマンドをカードアプリケーションに送信する（ステップ904）。

REQ__AREA__INFOコマンドを受信したカードアプリケーションAP1は、処理905を実行する。この処理905の詳細については、図15のフローチャートを参照して説明する。

カードアプリケーションAP1は、DATA2よりDATA1を抽出し、カ
25 ードアプリケーションAP1が保持する秘密鍵PriSで復号化し、乱数Rh
とファイル名FILE3を得る（ステップS9051）。

次に、DATA2より公開鍵を識別して識別子Info_PubHを抽出し、

Info__PubHが示す公開鍵PubHに対応付けられた端末200によるアクセスが認められているかを、ファイルFILE3のアクセス権限設定を参照して確認する。権限がなければ、その旨のエラーをレスポンスAPDUとして端末200に返す。アクセスする権限があれば、FILE3のファイルサイズSIZE3を取得する（ステップS9052）。

次に、乱数Rsを生成し（ステップS9053）、ファイルFILE3に対する端末200からのセキュリティ保護領域アクセスコマンドによるアクセスが可能となるように、図47で示すアクセス有効テーブル4500への登録を行い、端末200がセキュリティ保護領域アクセスコマンドを用いてアクセスするときに使用するためのエリア番号XをファイルFILE3に割り当て、ファイルサイズSIZE3とともにエリア・セッション鍵管理部111に記憶する（ステップS9054）。このエリア番号とは、端末200がセキュリティ保護領域アクセスコマンドによるアクセスを行うときに、アクセス領域指定コマンドによって送信するアクセス領域指定情報に含める情報をいう。

次に、乱数Rs、エリア番号X、ファイルサイズSIZE3を結合し、DATA3を生成し（ステップS9055）、DATA3を端末200の公開鍵PubHで暗号化してDATA4を生成する（ステップS9056）。

次に、乱数Rsと乱数Rhに排他的論理和を施し、乱数Rを生成し（ステップS9057）、乱数Rから暗号用セッション鍵Kd、検証用セッション鍵Kmを生成する（ステップS9058）。

次に、セッション鍵Kd及びKmをエリア番号Xと関連付け、エリア・セッション鍵管理部111に記憶する（ステップS9059）。

図13に戻り、カード100はここまでの処理を終えると端末200にDATA4を含んだレスポンスAPDUを端末200に送信する（ステップ906）。

レスポンスAPDUを受信した端末200は、レスポンスAPDUからDATA4を抽出し、処理907を実行する。この処理907の詳細については、

図16のフローチャートを参照して説明する。

端末200は、端末200の秘密鍵Pr i Hを用いてDATA4を復号しDATA3を取得する（ステップS9071）。次に、端末200は、DATA3より乱数Rsを取得し、乱数Rsと乱数Rhに排他的論理和を施し、乱数R5を生成し（ステップS9072）、乱数Rから暗号用セッション鍵Kd、検証用セッション鍵Kmを生成する（ステップS9073）。

以上のステップ901から907を踏むことで、端末200とカード100間の相互認証を行い、かつ端末200が指定したファイルに対するアクセス権があれば端末200からのアクセスが可能な状態となり、またアクセスする際に必要なエリア番号、エリア番号に割り当てられたファイルのサイズSIZE3、および検証用セッション鍵Km、暗号用セッション鍵Kdを共有することができる

なお、ステップ904において端末200からカード100に伝えられるファイル名は、カードアプリケーションが管理するファイルを直接示すものである必要はなく、カードアプリケーションがどのファイルを指しているかが認識できる形であればよい。

また、端末200がアクセスしたいファイル及びステップS9054において、そのファイルに対して端末200がアクセス可能となる設定を行った際に割り当てられるエリア番号が常に同じとなるようにし、これらの情報を端末200とカード100間であらかじめ認識しておくことで、ステップ904における端末200がアクセスしたいファイル名の通知およびステップ906におけるファイルに割り当てられたエリア番号の通知を省略することもできる。

さらに、本説明では、各カードアプリケーションが図12で示すようにディレクトリとファイルからなる階層構造をもち、ディレクトリ名およびファイル名でデータを管理している形態で説明したが、カードアプリケーションに割り当てられた領域を適当な大きさに分割し、分割されたそれぞれの領域に番号のような識別子を割り当てて管理する形態でもよい。その場合は、図13で示し

た処理手順で用いられるファイル名 F I L E 3 の代わりに前記識別子を用いる。

次に、端末 2 0 0 からセキュリティ保護領域に対してアクセスを行う際の処理について図 1 7 及び図 3 を用いて説明する。図 1 7 の実線は CMD ライン 2

5 2、点線は D A T 0 ライン 2 7 における転送を表す。

まず、端末 2 0 0 はカード 1 0 0 に対してメモリカードコマンドであるアクセス領域指定コマンドを送信する（ステップ 1 3 0 1）。このアクセス領域指定コマンドは、図 9 で示されるフォーマットとなっており、6 ビットのコマンドコード 4 0 1 と 3 2 ビットのコマンド引数 4 0 2 から構成される。

10 アクセス領域指定コマンドにおけるコマンド引数 4 0 2 は、図 1 8 で示すように、D A T 0 ライン 2 7 に入力するデータがアクセス領域指定情報であることを示すフラグ 1 4 0 1 と送信データ数を示す 1 4 0 3 とからなる。フラグ 1 4 0 1 及び送信データ数 1 4 0 3 を合わせて 3 2 ビットに満たない場合は未使用フィールド 1 4 0 2 が存在する。

15 D A T 0 ライン 2 7 に入力するデータは、5 1 2 バイト単位となっており、送信データ数 1 4 0 3 は、この 5 1 2 バイト単位の入力を何回行うかを示す。

次に、カード 1 0 0 のコマンド受信部 1 0 1 は、端末 2 0 0 から送信されたコマンドを受信し、それがアクセス領域指定コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部 1 0 3 に対して、アクセス領域指

20 定コマンドを受信したことを通知する（ステップ 1 3 0 2）。

次に、端末 2 0 0 はカード 1 0 0 の CMD ライン 2 2 からアクセス領域指定コマンドに対するレスポンスを受信し、D A T 0 ライン 2 7 に図 2 1 で示すフォーマットでアクセス領域指定情報 1 7 0 2 を入力する（ステップ 1 3 0 3）。

図 2 1 の 1 7 0 1 で示される長さは、後に続くアクセス領域指定情報 1 7 0 2 の長さを示している。長さフィールド 1 7 0 1 とアクセス領域指定情報 1 7 0 2 の合計長に合わせてコマンド引数 4 0 2 の送信データ数 1 4 0 3 が設定されている。また、前記合計長は必ずしも 5 1 2 バイトの倍数になるわけでは

ないので、512バイトの倍数になるようにパディング1703を付加する。

アクセス領域指定情報1702は、図22で示されるように、図13のステップ906でカードから通知されたエリア番号Xを指定するエリア番号1801と、0以上であり、同じくカードから通知されたファイルサイズSIZE
5 3の範囲で選択可能なアクセス開始アドレス1802と、1以上であり、（ファイルサイズSIZE3-アクセス開始アドレス1802）の範囲で選択可能なアクセスデータサイズ1803とで構成される。

次に、カード内部のデータ送受信部102は、端末から入力されたアクセス領域指定情報1702を受信するとともに、データ制御部103にアクセス領
10 域指定情報1702を受信したことを通知する。

次に、データ制御部103は、データ送受信部102からアクセス領域指定情報1702を読み出し、エリア番号1801が、図15のステップS905
4にて割り当てられたエリア番号Xであるか、アクセス開始アドレス及びアクセスデータサイズは、エリア番号Xと対応したファイルのファイルサイズ範囲
15 に収まっているかをチェックし、異常があればカード内部に保持するエラーフラグをONに設定する。

データ制御部103は、異常がなければ、図3に示すパラメータ記憶部109にアクセス領域指定情報1702（具体的にはエリア番号1801、アクセス開始アドレス1802、アクセスデータサイズ1803）を記憶する。

20 以上が、アクセス領域を指定する処理である。

次に、図10のセキュリティ保護領域61に対して読み出しを行う際の処理について説明する。

図17において、端末200は、カード100に対してセキュリティ保護領域読み出しコマンドを送信する（ステップ1304）。このセキュリティ保護
25 領域読み出しコマンドは、図8で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

セキュリティ保護領域読み出しコマンドにおけるコマンド引数402は、セキュリティ保護領域読み出しコマンドを送信した端末が、アクセス領域指定コマンドを送信した端末200と同一であるか、またセッション鍵共有手順を経てエリア番号Xが示す領域に対するアクセス権限があることを確認された端末200と同一であるかを検証するための検証データからなる。

この検証データの生成方法について図23を用いて説明する。

アクセス領域指定情報1702は、アクセス領域指定コマンドにおいてDATライン27に入力するパラメータである。検証鍵2101は、図13のステップ907で生成した検証用セッション鍵Kmである。

10 端末200内部の検証データ生成部203は、暗号演算を行うモジュールであり、セキュリティ保護領域アクセス（読み出しまたは書き込み）コマンドに含める検証データを生成する。ここでは、DES-MACと呼ばれるMAC（Message Authentication Code）生成処理を行う。アクセス領域指定情報1702に対してパディングデータ2105を付加した2102を入力データとして、検証鍵2101を用いてDES暗号を用いたMAC生成処理を行い、MACデータを検証データ2104として作成する。

15 パディングデータ2105については、端末200からカード100に対してアクセス領域指定コマンドを送信するときにアクセス領域指定情報1702と併せて送信してもよいし、あらかじめ端末とカードの間で取り決めをしたパディング生成ルールに基づいて生成したパディングデータを付与してもよい。

なお、本実施の形態ではDES-MACを用いて検証データを作成しているが、他のアルゴリズムを用いてもよい。さらに、用途に応じて検証アルゴリズムを選択可能としても良い。

25 なお、端末200が正当であるか認証する必要がなく、アクセス領域指定コマンドとの対応付けのみ確認したい場合は、暗号処理を用いずに、単にSHA1（Secure Hash Algorithm 1）やMD5（Message Digest 5）アルゴリズム

を用いたハッシュデータを検証データとして用いてもよい。

端末200は、上記の検証データ生成処理によって32ビットの検証データを生成し、セキュリティ保護領域読み出しコマンドの引数として使用する。

次に、カード100のコマンド受信部101は、端末200から送信された
5 コマンドを受信し、それがセキュリティ保護領域読み出しコマンドであることを認識し、アクセス領域指定情報1702に関するエラーフラグがONに設定されている場合は、レスポンスとしてエラーを返す。また、アクセス領域指定情報1702に関するエラーフラグがONに設定されていない場合は、図15
10 で示すように、端末に正常レスポンスを返す（ステップ1305）とともに、データ制御部103に対してセキュリティ保護領域読み出しコマンドを受信したことを通知し、パラメータ検証部108にコマンド引数402として与えられた検証データ2104を渡す。

次に、端末200は、カード100のCMDライン22からセキュリティ保護領域読み出しコマンドに対するレスポンスを受信し、DAT0ライン27か
15 らデータが出力されるのを待つ。

以降にカード100によるセキュリティ保護領域のデータ出力処理について説明する。

カード100のパラメータ検証部108は、パラメータ記憶部109からアクセス領域指定コマンドによって端末200から与えられ、記憶しておいたア
20 クセス領域指定情報1702を読み出し、アクセス領域指定情報1702に含まれるエリア番号X（1801）に対応する、図15のステップS9059で記憶した検証用セッション鍵Kmをエリア・セッション鍵管理部111から取得する。

次に、カード100のパラメータ検証部108は、検証用セッション鍵Km
25 とアクセス領域指定情報1702を用いて、図24に示した検証データ生成処理を行い、検証データ1904を生成する。なお、検証データ生成処理については、図23で示した端末200による検証データ生成処理と同様であるので

詳細な説明は省略する。

次に、カード100のパラメータ検証部108は、上記検証データ生成処理で生成した検証データ1904と、端末200からセキュリティ保護領域読み出しコマンドの引数によって与えられた検証データ504を比較し、一致しなければエラーとし、データ読み出し処理に移行しない。一致した場合は、次のデータ読み出し処理に移行することをデータ制御部103に通知する。

次に、カード100のデータ制御部103は、パラメータ記憶部109からアクセス領域指定情報1702を読み出し、その中に含まれるエリア番号Xを取得し、エリア・セッション鍵管理部111からエリア番号に対応するファイルFILE3を認識する

次に、カード100のデータ制御部103は、ファイルFILE3がアプリケーションAP1用の領域であることを確認し、格納用暗号鍵Ks__1を取得する。

次に、カード100のデータ制御部103は、アクセス領域指定情報1702からアクセス開始アドレス1802とアクセスデータサイズ1803を取得し、ファイルFILE3として管理されている領域に対して、アクセス開始アドレス1802をオフセット、アクセスデータサイズ1803を読み出しサイズとしてメモリアクセス部104にデータ読み出し要求を行う。

次に、カード100のデータ制御部103は、暗復号部107に対して、メモリアクセス部104によって読み出されたデータを格納用暗号鍵Ks__1で復号化するよう要求する。

次に、カード100のデータ制御部103は、暗復号部107に対して、暗復号部107によって復号化されたデータを暗号用セッション鍵Kdで暗号化するよう要求する。

次に、カード100のデータ制御部103は、データ送受信部102に対して、暗復号部107によって暗号用セッション鍵Kdで暗号化されたデータを端末200に送信するよう要求する。

上記の処理によって、カード100からセキュリティ保護領域のデータがセッション鍵Kdによって暗号化された状態で出力可能となる。

端末200は、カード100からデータが出力可能となったことを認識し、
図17に示すように、DAT0ライン27からセッション鍵Kdによって暗号
5 化された状態のデータを取得し（ステップ1306）、端末が保持する暗号用
セッション鍵Kdによってデータを復号化し、アクセス領域指定情報1702
で指定した領域のデータを得る。

次に、セキュリティ保護領域に対して書き込みを行う際の処理について、図
25を参照して説明する。

10 端末200からのアクセス領域指定コマンドの送信（ステップ2001）、
前記コマンドに対するカード100からのレスポンス（ステップ2002）、
及びアクセス領域指定情報の送信（ステップ2003）については、それぞれ
図17に示したセキュリティ保護領域に対する読み出し処理におけるステッ
プ1301～1303と同様であるので、説明を省略する。ステップ2001
15 ～ステップ2003を行った後、端末200は、カード100に対してセキュ
リティ保護領域書き込みコマンドを送信する（ステップ2004）。このセキュ
リティ保護領域書き込みコマンドは、図8で示されるフォーマットとなっ
ており、6ビットのコマンドコード401と32ビットのコマンド引数402か
ら構成される。

20 セキュリティ保護領域読み出しコマンドにおけるコマンド引数402は、セ
キュリティ保護領域読み出しコマンドを送信した端末200が、アクセス領域
指定コマンドを送信した端末200と同一であるか、また、セッション鍵共有
手順を経てエリア番号Xが示す領域に対するアクセス権限があることを確認
された端末200と同一であるかを検証するための検証データ1904から
25 なる。

この検証データの生成方法についてはセキュリティ保護領域読み出しコマ
ンドと同様であるため、詳細な説明は省略する。

端末200は、検証データ生成処理によって32ビットの検証データを生成し、セキュリティ保護領域書き込みコマンドの引数として使用する。

- 次に、カード100のコマンド受信部101は、端末200から送信されたコマンドを受信し、それがセキュリティ保護領域書き込みコマンドであることを認識し、アクセス領域指定情報1702に関するエラーフラグが設定されている場合は、レスポンスとしてエラーを返す。

- また、アクセス領域指定情報1702に関するエラーフラグが設定されていない場合は、CMDライン22から端末200に対して正常レスポンスを返す(ステップ2005)とともに、データ制御部103に対してセキュリティ保護領域書き込みコマンドを受信したことを通知し、パラメータ検証部108にコマンド引数として与えられた検証データ504を渡す。

- 次に、端末200は、カード100のCMDライン22からセキュリティ保護領域書き込みコマンドに対するレスポンスを受信し、DAT0ライン27にデータの入力を行う。ここでDAT0ライン27に入力するデータは、図13のステップ907で生成した暗号用セッション鍵Kdで暗号化したものである。また、入力データサイズは、アクセス領域指定情報1702で指定したアクセスデータサイズと同一である。

以降にカードによるセキュリティ保護領域へのデータ格納処理について説明する。

- カード100のパラメータ検証部108は、パラメータ記憶部109からアクセス領域指定コマンドによって端末200から与えられ、記憶しておいたアクセス領域指定情報1702を読み出し、アクセス領域指定情報1702に含まれるエリア番号X(1801)に対応する、図15のステップ9059で記憶した検証用セッション鍵Kmをエリア・セッション鍵管理部111から取得する。

次に、カード100のパラメータ検証部108内部の検証データ生成部1903は、検証用セッション鍵Kmとアクセス領域指定情報1702を用いて、

図 2 4 に示した検証データ生成処理を行い、検証データ 1 9 0 4 を生成する。
なお、検証データ生成処理については、図 2 3 で示した端末による検証データ
生成処理と同様であるので詳細な説明は省略する。

次に、カード 1 0 0 のパラメータ検証部 1 0 8 は、上記で生成した検証デー
5 タ 1 9 0 4 と、端末 2 0 0 からセキュリティ保護領域書き込みコマンドの引数
によって与えられた検証データ 2 1 0 1 を比較し、一致しなければエラーとし、
データ書き込み処理に移行しない。一致した場合は次のデータ書き込み処理に
移行することをデータ制御部 1 0 3 に通知する。

次に、カード 1 0 0 のデータ制御部 1 0 3 は、パラメータ記憶部 1 0 9 から
10 アクセス領域指定情報 1 7 0 2 を読み出し、その中に含まれるエリア番号 X を
取得し、エリア・セッション鍵管理部 1 1 1 からエリア番号に対応するファイ
ル F I L E 3 を認識する。

次に、カード 1 0 0 のデータ送受信部 1 0 2 は、端末 2 0 0 から入力された
データを受信する。

15 次に、カード 1 0 0 のデータ制御部 1 0 3 は、ファイル F I L E 3 がアプリ
ケーション A P 1 用の領域 7 1 の中に存在することから、アプリケーション A
P 1 用領域 7 1 に対応した格納用暗号鍵 K s _ 1 を取得する。

次に、カード 1 0 0 のデータ制御部 1 0 3 は、暗復号部 1 0 7 に対して、デ
ータ送受信部 1 0 2 が受信したデータを暗号用セッション鍵 K d で復号化す
20 るよう要求する。

次に、カード 1 0 0 のデータ制御部 1 0 3 は、暗復号部 1 0 7 に対して、暗
復号部 1 0 7 が復号化したデータを格納用暗号鍵 K s _ 1 で暗号化するよう
要求する。

次に、カード 1 0 0 のデータ制御部 1 0 3 は、アクセス領域指定情報 1 7 0
25 2 からアクセス開始アドレス 1 8 0 2 とアクセスデータサイズ 1 8 0 3 を取
得し、ファイル F I L E 3 として管理されている領域に対し、アクセス開始ア
ドレス 1 8 0 2 をオフセット、アクセスデータサイズ 1 8 0 3 を書き込みサイ

ズとして、メモリアクセス部 104 に対してデータ書き込み要求を行う。

上記のようにして、端末 200 が入力したセッション鍵 K_d で暗号化されたデータを格納鍵 K_s__1 で暗号化してフラッシュメモリ 105 に格納する。

本実施の形態では、セッション鍵の共有と、アクセス可能領域に関する情報
5 の共有を 1 つのコマンドで同時に行っているが、別コマンドとして行ってもよい。

本実施の形態では、セッション鍵の共有と、アクセス可能領域に関する情報の共有を 1 つのコマンドで同時に行っているが、別コマンドとして行ってもよい。

10 以上、本発明のように、IC カード用コマンドとメモリアクセス用コマンドを受信可能なメモリカードにおいて、カードアプリケーションが利用し、通常はカードアプリケーション経由でのみアクセス可能であり、端末からのアクセスが制限されているセキュリティ保護領域に対して、カードアプリケーション
と端末が相互認証し、カードアプリケーションがアクセス可能設定を行うこと
15 により、端末からメモリアクセス用コマンドを用いてアクセスすることが可能となる。

また、カードアプリケーションがアクセス可能設定を行うためのカードアプリケーションと端末間の相互認証は、用途が限定されたメモリアクセス用コマンドではなく、IC カード用コマンドを使うことにより、データのセキュリティ
20 レベルに応じて相互認証方式を柔軟に選択可能となる。

また、メモリアクセス用コマンドに含まれる引数サイズが 32 ビットのよう
に小さい場合でも、本発明のように、アクセス領域指定とセキュリティ保護
領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマン
ドに検証データを含めることで、アクセス領域指定を行った端末アプリケー
25 ションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケー
ションと検証用鍵を保持した端末アプリケーションが同一であることをカー
ドが検証することが可能となる。

また、検証用及び暗号用セッション鍵の共有処理をセキュリティ保護領域アクセスのたびに行うことにより、セキュリティ保護領域アクセスに含める検証データとして適当な値を設定して繰り返し不正アクセスを行う攻撃に対する防御性を高めることができる。

- 5 また、端末からアクセスしたいファイルをカードに通知し、それにエリア番号を割り当て、カードから端末に通知することにより、端末がアクセス可能な領域を設定することが可能となる。また、複数のファイルに対して行うことにより、同時に複数のファイルに対してアクセス可能な状態を作ることができる。

（実施の形態２）

- 10 本実施の形態では、端末が、領域指定コマンドで指定するエリア番号をあらかじめ認識している場合のシーケンスを説明する。

まず、カード内モジュール構成について図 2 6 を用いて説明する。なお、図 2 6 のカード 5 0 0 の端子構成は、図 4 に示したものと同様であるため、その図示及び説明は省略する。

- 15 カード 5 0 0 内モジュールは、CMDラインに接続され、コマンドの受信及びレスポンスの送信を行う処理命令受信手段 5 0 1 と、データを格納する記憶領域 5 0 6 と、記憶領域 5 0 6 へのアクセス処理を行う記憶領域アクセス手段 5 0 5 と、DATラインに接続され、記憶領域アクセス手段 5 0 5 が読み出したデータを外部機器に送信するデータ送信手段 5 0 2 と、同じくDATライン
20 に接続され、外部機器からデータを受信するデータ受信手段 5 0 3 と、処理命令受信手段 5 0 1 が受け取った指定情報を検証する指定情報検証手段 5 0 4 と、からなる。

次に、端末 6 0 0 内モジュール構成について、図 2 7 を用いて説明する。

- 25 端末 6 0 0 内モジュールは、カード 5 0 0 に対するコマンド送信と、レスポンス受信を行う処理命令送信手段 6 0 4 と、カード 5 0 0 に対するデータ送信を行うデータ送信手段 6 0 5 と、カード 5 0 0 からのデータ受信を行うデータ受信手段 6 0 6 と、アクセスする領域を決定する指定情報決定手段 6 0 1 と、指定情

報から検証情報を生成する検証情報生成手段602と、カード500に送信するデータ及びカード500から受信するデータを格納するデータ記憶手段603と、からなる。

次に、端末600からカード500のセキュリティ保護領域に対してアクセスを行う際の処理について、上記図26及び図27と、図28に示すフローチャートを用いて説明する。

まず、端末600は指定情報決定手段601にてリードアクセス又はライトアクセスを行う領域を決定し（ステップS2601）、アクセス領域指定情報を生成する（ステップS2602）。次に、このアクセス領域指定情報をデータ記憶手段603に格納して領域指定命令を処理命令送信手段604からカード500に送信する（ステップS603）。

領域指定命令のデータ部の一例を図29に示す。

DATライン27に入力するデータは512バイト単位となっており、領域指定命令のデータ部は、アクセス領域指定情報2702の長さフィールド2701と、アクセス領域指定情報フィールド2702の合計長が512バイトに満たない場合、パディング2703が追加される。本実施の携帯では、長さフィールド2701は2バイトの長さを持ち、アクセス領域指定情報2702は、図30に示すように、1バイトのエリア番号2801、3バイトのアクセス開始アドレス2802、及び3バイトのアクセスデータサイズ2803からなる。つまり合計9バイトであり512バイトに満たないため、503バイトのパディング2703が付加される。

次に、図28に戻り、カード500は、処理命令受信手段501にて領域指定命令を受信すると（ステップS2604）、指定情報検証手段504にてアクセス領域指定情報2702を確認し、指定した領域が正しいかどうかをエリア番号2801に対応する領域が存在するか、アクセス開始アドレス2802及びアクセスデータサイズ2803がエリア番号2801で示された領域の範囲に収まっているかを元に判断する（ステップS2605）。指定情報検証

手段504は、指定した領域が正しくなければ、領域指定命令を無効として扱う（ステップS2606）。指定した領域が正しい場合、アクセス領域指定情報2702を保存し、アクセス領域指定情報2702と、端末600とカード500の間で共有している鍵を用いて、比較情報を生成する（ステップS2607）。

比較情報の生成方法の一例を図29に示す。

検証データ生成部2902は暗号演算を行うモジュールであり、本実施の形態ではDES-MACと呼ばれるMAC（Message Authentication Code）を生成する処理を行う。入力は、領域指定命令のデータ部2704と、端末600との間で共有している検証用の鍵2901である。DES-MACの出力結果は64ビットであるが、本実施の形態では、比較対象となる端末600から送信される検証情報が32ビットであるため、その出力を切り詰めた2903である前半32ビットのみを比較情報2904として用いる。なお、検証用鍵2901は、エリア番号に対応して個別かつ固定の鍵であってもよいし、エリア番号によらず1つの鍵であってもよい。

また、図32に示すように、カード700内部に検証用鍵共有手段701を備え、図33に示すように端末800内部に検証用鍵共有手段801を備え、カード700と端末800の間で、セキュリティ保護領域へのアクセスを行うたびに検証用鍵を変更してもよい。なお、図32及び図33の各構成において、図26及び図27に示した構成と同一部分には同一符号を付している。

次に、検証用鍵の共有方法について上記図32及び図33と、図34に示すシーケンスおよび図35に示す検証用鍵生成方法を用いて説明する。

図34において、端末800は検証用鍵共有手段801において、乱数R_aを生成し、この乱数R_aを含んだセッション鍵共有要求コマンドAPDUを作成し、処理命令送信手段604からAPDU送信コマンドをカード700に送信するとともに（ステップS3201）、データ送信手段605からセッション鍵共有要求コマンドAPDUをカード700に送信する（ステップS320

2)。

次に、カード700は処理命令受信手段501にてAPDU送信コマンドを端末800から受信し、データ受信手段503にて端末800から受信したセッション鍵共有要求コマンドAPDUを検証用鍵共有手段701に渡す。

- 5 検証用鍵共有手段801では、乱数R_bを生成し、図35に示すように、端末800から受信した乱数R_aと乱数R_bを結合したものに対し、あらかじめ端末800との間で共有しているマスター鍵Kを用いて暗号化処理(DES-MAC処理)を行い、セッション鍵Rを生成する。次に、カード700は、乱数R_bを含むレスポンスAPDUを生成する。

- 10 次に、端末800は、処理命令送信手段604からAPDU受信コマンドをカード700に送信する(ステップS3203)。

次に、カード700は、処理命令受信手段501にてAPDU受信コマンドを端末800から受信し、先ほど作成した乱数R_bを含むレスポンスAPDUをデータ送信手段502より端末800に送信する(ステップS3204)。

- 15 次に、端末800は、データ受信手段606によりレスポンスAPDUをカード700から受信し、検証用鍵共有手段801に渡す。検証用鍵共有手段801は、図35に示すように、先ほど自身が生成した乱数R_aと、レスポンスAPDUに含まれる乱数R_bを結合したものに対し、あらかじめカード700との間で共有しているマスター鍵Kを用いて暗号化処理(DES-MAC処理)を行
- 20 い、セッション鍵Rを生成する。

以上が、セキュリティ保護領域へのアクセスを行うたびにセッション鍵を変更する場合の、端末800とカード700の間における検証用鍵共有手順である。

- 25 なお、本実施の形態ではDES-MACを用いているが、当然他の暗号アルゴリズムを用いてもよい。また、端末800が正当であるか、つまり同一の鍵を持っているかを検証する必要がある場合、例えば、領域指定命令のアクセス領域指定情報2702が端末の意図したものになっているかの検証のみ行う

場合は、暗号処理を用いずに、図 3 6 に示すような検証データ生成部 3 4 0 1 にて S H A - 1 演算や、M D 5 アルゴリズムを用いたハッシュ演算やチェックサム演算の結果を比較情報として用いることができる。これらのアルゴリズムを用いた場合も、比較対象が 3 2 ビット長ならば、出力結果を切りつめ 3 4 0 5 2、その一部の 3 2 ビットのみを比較情報 3 4 0 3 とする。

次に、図 2 8 に戻り、端末 8 0 0 は、検証データ生成部にてアクセス領域指定情報 2 7 0 2 と、端末 8 0 0 とカード 7 0 0 の間で共有している検証用鍵 2 9 0 1 から検証情報を生成する（ステップ S 2 6 0 8）。

この検証情報の生成について、図 3 7 に示す。検証情報生成部 3 5 0 2 にて
10 検証用鍵 3 5 0 1 と領域指定命令のデータ部 2 7 0 4 を用いて暗号処理を行い、検証情報 3 5 0 4 を生成する。生成方法は、図 3 1 で示したカード 7 0 0 における比較情報 2 9 0 4 の生成方法と全く同じである。

次に、図 2 8 に戻り、端末 8 0 0 は、生成した検証情報 3 5 0 4 をアクセス命令（読み出し）の引数に載せて、処理命令送信手段 6 0 4 からアクセス命令
15 を送信する（ステップ S 6 0 9）。

アクセス命令は、図 3 8 で示すフォーマットとなっており、コマンドコード 3 6 0 1 とコマンド引数 3 6 0 2 の長さはそれぞれ 6 ビットと 3 2 ビットである。アクセス命令では、コマンド引数 3 6 0 2 に検証情報 3 5 0 4 を格納する。

20 次に、図 2 8 に戻り、カード 7 0 0 は、処理命令受信手段 5 0 1 にてアクセス命令（読み出し）を受信し（ステップ S 2 6 1 0）、指定情報検証手段 5 0 4 にて事前に領域指定命令が正常に完了したかどうかを確認する（ステップ S 2 6 1 1）。領域指定命令が未受信である、又は指定した領域が正しくないなどの理由で正常に完了していない場合は、アクセス命令をエラーとして端末 8
25 0 0 に通知する（ステップ S 2 6 1 2）。この時、端末 8 0 0 は、カード 7 0 0 からエラーを受信する（ステップ S 2 6 1 2 A）。

事前に領域指定命令が正常に完了している場合、指定情報検証手段 5 0 4 は、

先ほどカード 700 が作成した比較情報 2904 と、アクセス命令のコマンド
引数に格納された検証情報 3504 を比較する（ステップ S2613）。比較
の結果、検証情報 3504 が不正であったならば、アクセス命令をエラーとし
て端末 800 に通知する（ステップ S2614）。この時、端末 800 は、カ
ード 700 からエラーを受信する（ステップ S2614A）。検証情報が正常
であったならば、指定情報検証手段 5044 は記憶領域アクセス手段 505 に
アクセス領域指定情報 2702 を通知し、記憶領域アクセス手段 505 は記憶
領域 506 内のアクセス領域指定情報 2702 で指定された領域からデータ
を読み出し、データ送信手段 502 からデータを端末 800 に送信する（ステ
ップ S2615）。

次に、端末 800 は、カード 700 から送信された読み出しデータをデータ
受信手段 606 にて受信し（ステップ S2616）、データ記憶手段 603 に
格納する。

以上の通り、メモリアクセス用コマンドに含められる引数サイズが 32 ビッ
トのように小さい場合でも、本発明のように、アクセス領域指定とセキュリテ
ィ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用の
コマンドに検証データを含めることで、アクセス領域指定を行った端末アプリ
ケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリ
ケーションと検証用鍵を保持した端末アプリケーションが同一であること
をカードが検証することが可能となる。

なお、検証データ生成のために、領域指定情報と検証用鍵に加え、カードか
ら出力される乱数情報を利用する方法を、図 39 に示すシーケンスを用いて以
下に説明する。なお、図 39 に示す各ステップにおいて、図 28 に示したシー
ケンスのステップと同一のステップには同一符号を付して、その説明は省略す
る。

図 39 に示すように、端末 800 から乱数取得命令を端末 800 からカード
700 に送信し（ステップ S3701）、カード 700 が乱数 T を生成し、この

乱数 T をカード 700 内部の指定情報検証手段 504 に保持するとともに、データ送信手段 502 から端末 800 に送信する（ステップ S3702）。端末 800 は、カード 700 から送信された乱数 T をデータ受信手段 606 にて受信する（ステップ S3703）。

- 5 乱数 T を検証情報生成処理に利用する場合のカード 700 における比較情報の生成処理（ステップ S2607）、および、端末 800 における検証情報の生成処理（ステップ S2608）は、それぞれ図 40 および図 41 で示すように、乱数 T と領域指定命令のデータ部 2704 を結合したものに対して暗号処理を行い、比較情報 3804 及び検証情報 3904 を出力する。

- 10 以上のように、検証情報生成に乱数情報を利用することにより、同一の領域指定情報と検証用鍵を用いて検証情報を作成しても、乱数情報が変化することで出力される検証情報が変化するため、よりセキュリティ強度を向上させることができる。

（実施の形態 3）

- 15 本実施の形態では、鍵の共有処理を含むシーケンスの例を説明する。

まず、カード内モジュール構成について図 42 を用いて説明する。なお、カードの端子構成は、図 4 に示したものと同様であるため、その図示及び説明は省略する。

- カード内モジュールは、CMDラインに接続され、コマンドの受信及びレスポンスの送信を行う処理命令受信手段 901 と、データを格納する記憶領域 906 と、記憶領域 906 へのアクセス処理を行う記憶領域アクセス手段 905 と、DATラインに接続され、記憶領域アクセス手段 905 が読み出したデータを外部機器に送信するデータ送信手段 902 と、同じく DATラインに接続され、外部機器からデータを受信するデータ受信手段 903 と、端末 1000 との間でセキュリティ保護領域アクセスコマンドによるアクセスが可能な領域に関する情報を共有する可能領域情報共有部 907 と、データ受信手段 903 経由して受け取った指定情報を、検証用鍵を用いて検証する指定情報検証手
- 20
- 25

段 904 と、からなる。

次に、端末内モジュール構成について、図 43 を用いて説明する。

端末内モジュールは、カード 900 に対するコマンド送信と、レスポンス受信を行う処理命令送信手段 1004 と、カード 900 に対するデータ送信を行うデータ送信手段 1005 と、カード 900 からのデータ受信を行うデータ受信手段 1006 と、アクセスする領域を決定する指定情報決定手段 1001 と、セキュリティ保護領域アクセスコマンドによるアクセスが可能な領域に関する情報を共有する可能領域情報共有部 1007 と、指定情報から検証情報を生成する検証情報生成手段 1002 と、カード 900 に送信するデータ及びカード 900 から受信するデータを格納するデータ記憶手段 1003 と、からなる。

次に、端末 1000 からカード 900 内のセキュリティ保護領域に対してアクセスを行う際の処理について、上記図 42 及び図 43 と、図 44 及び図 45 に示すシーケンスを用いて説明する。

まず、端末 1000 は、指定情報決定手段 1001 にて、リードアクセス又はライトアクセスを行う領域 A を決定し（ステップ S4201）、可能領域情報共有部 1007 にて、前記領域 A に対するセキュリティ保護領域アクセスコマンドによるアクセスを許可するように要求するコマンド APDU である領域開放要求コマンドを処理命令送信手段 1004 からカード 900 に送信する（ステップ S4202）。領域開放要求コマンドは、端末 1000 の公開鍵を表す識別子 `Info_PubH` と、領域 A を示す識別子 `a` をカード 900 の公開鍵 `PubS` で暗号化したデータとを含む。なお、コマンド APDU の送信方法は実施の形態 1 で説明した方法と同様であるので、詳細な説明は省略する。

次に、領域開放要求コマンドを受信したカード 900 は、可能領域情報共有手段 907 にてコマンドに含まれる暗号化データをカード 900 自身の秘密鍵 `PriS` で復号化する（ステップ S4203）。次いで、端末 1000 の公開鍵識別子 `Info_PubH` からコマンドを送信した端末 1000 を識別し、識別子 `a` で示される領域 A のアクセス権限を参照することで、該端末 10

00が領域Aに対するアクセスを許可されているかどうかを確認する（ステップS4205）。

アクセスが許可されていない場合は、領域開放失敗を示すデータをレスポンスAPDUとしてデータ送信手段902から端末1000に送信する（ステップS4206）。アクセスが許可されている場合は、領域Aの識別子aと領域Aに割り当てたエリア番号Xを、指定情報検証手段904内に持つ、セキュリティ保護領域アクセスコマンドによるアクセス可否を設定するアクセス有効テーブル4400（図46参照）に登録する（ステップS4207）。次に、領域Aに対応した検証用鍵Rをアクセス有効テーブル4400に登録する（ステップS4208）。

次に、エリア番号X、領域Aのサイズを端末1000の公開鍵PubHで暗号化し、レスポンスAPDUとしてデータ送信手段902から端末1000に送信する（ステップS4209）。

次に、端末1000は、APDU受信コマンドを処理命令送信手段1004からカード900に送信し、データ受信手段1006を用いてレスポンスAPDUをカード900から取得する（ステップS4210）。なお、レスポンスAPDUの取得方法は実施の形態1で説明した方法と同様であるので、詳細な説明は省略する。

次に、端末1000の可能領域情報共有手段1007は、レスポンスAPDUに含まれる暗号データを端末1000自身の秘密鍵PriHで復号化し（ステップS4211）、エリア番号X、エリア番号Xで示される領域Aのサイズを得る。次に、端末1000は領域Aに対応したセッション鍵を検証情報生成手段1002に登録する。エリア番号Xはアクセス領域指定情報を生成するために指定情報決定手段1001に登録する（ステップS4212）。以後、図45のフローチャートに移行する。

次に、端末1000は指定情報決定手段1001にて可能領域情報共有手段1007によって登録されたエリア番号Xを用いてアクセス領域指定情報を

生成する（ステップS 4 2 1 3）。次に、このアクセス領域指定情報をデータ部2 7 0 4（図2 9 参照）に格納して、領域指定命令を処理命令送信手段1 0 0 4からカード9 0 0に送信する（ステップS 4 2 1 4）。なお、領域指定命令におけるアクセス領域指定情報は実施の形態2と同様であるので、詳細な説明は省略する。

次に、カード9 0 0は、処理命令受信手段9 0 1にて端末1 0 0 0から領域指定命令を受信すると（ステップS 4 2 1 5）、指定情報検証手段9 0 4にてアクセス領域指定情報を確認し、エリア番号Xがアクセス有効テーブル4 4 0 0に登録されているか、図3 0に示したアクセス開始アドレス2 8 0 2及びアクセスデータサイズ2 8 0 3を元に領域Aの範囲に収まっているか判断する（ステップS 4 2 1 6）。指定情報検証手段9 0 4は、指定した領域が正しくなければ、領域指定命令を無効として扱う（ステップS 4 2 1 7）。指定した領域が正しい場合、アクセス領域指定情報を保存し、アクセス領域指定情報とアクセス有効テーブル4 4 0 0に登録された領域Aに対応した検証用鍵Rを用いて、比較情報を生成する（ステップS 4 2 1 8）。なお、比較情報の生成方法は実施の形態2と同様であるので、詳細な説明は省略する。

次に、端末1 0 0 0は、検証情報生成手段1 0 0 2にてアクセス領域指定情報と、可能領域情報共有部1 0 0 7によって登録されたセッション鍵Rを用いて検証情報を生成し（ステップS 4 2 1 9）、アクセス命令（読み出し）の引数に載せて、処理命令送信手段1 0 0 1からアクセス命令をカード9 0 0に送信する（ステップS 4 2 2 0）。なお、検証情報の生成方法及びアクセス命令の送信方法は実施の形態2と同様であるので、詳細な説明は省略する。

次に、カード9 0 0は、処理命令受信手段9 0 1にてアクセス命令（読み出し）を受信し（ステップS 4 2 2 1）、指定情報検証手段9 0 4にて事前に領域指定命令が正常に完了したかどうかを確認する（ステップS 4 2 2 2）。領域指定命令が未受信である、又は指定した領域が正しくないなどの理由で正常に完了していない場合は、アクセス命令をエラーとして端末1 0 0 0に通知す

る（ステップS 4 2 2 3）。この時、端末1 0 0 0は、カード9 0 0からエラーを受信する（ステップS 4 2 2 3 A）。

事前に領域指定命令が正常に完了している場合、指定情報検証手段9 0 4は、先ほどカード9 0 0が作成した比較情報と、アクセス命令の引数に格納された
5 検証情報を比較する（ステップS 4 2 2 4）。比較の結果、検証情報が不正であったならば、アクセス命令をエラーとして端末1 0 0 0に通知する（ステップS 4 2 2 5）。この時、端末1 0 0 0は、カード9 0 0からエラーを受信する（ステップS 4 2 2 5 A）。

検証情報が正常であったならば、指定情報検証手段9 0 4は、記憶領域アクセス手段9 0 5に指定情報を通知し、記憶領域アクセス手段9 0 5は記憶領域
10 9 0 6内の領域指定命令で指定された領域からデータを読み出し、データ送信手段9 0 2からデータを端末1 0 0 0に送信する（ステップS 4 2 2 6）。

次に、端末1 0 0 0は、カード9 0 0から送信された読み出しデータをデータ受信手段1 0 0 6にて受信し、データ記憶手段1 0 0 3に格納する（ステップS 4 2 2 7）。
15

次に、端末1 0 0 0は、領域Aに対するセキュリティ保護領域アクセスコマンドによるアクセスが不要になったとき、領域Aに対応するエリア番号Xを無効化するための領域無効コマンドAPDUを作成し、データ送信手段1 0 0 5からカード9 0 0に送信する（ステップS 4 2 2 8）。

20 次に、領域無効コマンドAPDUを受信したカード9 0 0は、アクセス有効テーブル4 4 0 0を検索し、エリア番号Xが見つければ、テーブル内のエリア番号Xに割り当てられた領域識別子a、セッション鍵Rとともにエリア番号Xの登録を削除し、エリア番号Xを指定した領域Aへのセキュリティ保護領域アクセスコマンドによるアクセスを無効化する（ステップS 4 2 2 9）。

25 以上の通り、セキュリティ保護領域内のある領域に対し、必要な場合のみ領域開放要求によってセキュリティ保護領域アクセスコマンドによるアクセスが可能な状態にし、また不要となったときは領域無効要求によって、その領域

へのアクセスを不可能にすることで、セキュリティ強度を向上させることができる。

本明細書は、2003年7月16日出願の特願2003-275672及び
2004年7月2日出願の特願2004-197453に基づく。この内容は
5 すべてここに含めておく。

産業上の利用可能性

メモリカードコマンドとICカードコマンドを併用し、メモリアクセスにつ
いてはメモリカードコマンドを使用することで複雑さを回避しながら、少ない
10 コマンド引数でも安全に端末を認証可能とすることができる。

請求の範囲

1. 機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。
2. 機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。
3. 機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、検証用鍵を共有化するステップと、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

4. 機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記メモリデバイスとで、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

5. 機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

6. 機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、

前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

- 5 7. 機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。
- 10 8. 機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域
- 15 20 25

- を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法
9. 機器から読み書きされるメモリデバイスであって、アクセスする領域を指定する指定情報を受信するとともに、前記指定情報に基づく検証情報と読み出し又は書き込み命令を併せて受信する処理命令受信手段と、前記指定情報を、前記検証情報を用いて検証処理を行う指定情報検証手段と、データを格納する記憶領域と、前記検証処理が成功した場合に、前記処理命令に応じて、前記記憶領域の前記指定領域に対する読み出し又は書き込みを行う記憶領域アクセス手段と、前記記憶領域アクセス手段が読み出したデータを前記機器に送信するデータ送信手段と、前記機器から書き込みデータを受信するデータ受信手段と、を備えることを特徴とするメモリデバイス。
10. 前記指定情報検証手段の検証処理が、前記検証情報と検証用鍵を用いて行うことを特徴とする請求の範囲9記載のメモリデバイス。
11. 前記機器との間で前記検証用鍵を共有する検証用鍵共有手段をさらに備えることを特徴とする請求の範囲10記載のメモリデバイス。
12. 前記機器との間でメモリデバイスへのアクセス可能な領域を示す可能領域情報を共有する可能領域情報共有手段をさらに備えることを特徴とする請求の範囲9記載のメモリデバイス。
13. メモリデバイスを読み書きする情報機器であって、読み出し又は書き込みする領域を決定し、前記領域を指定する指定情報を決定する指定情報決定手段と、前記指定情報から前記検証情報の生成処理を行う検証情報生成手段と、前記指定情報の送信と、前記検証情報と読み出し又は書き込みの処理命令とを

併せて送信する処理命令送信手段と、前記処理命令が書き込みの場合は、前記メモリデバイスにデータを送信するデータ送信手段と、前記処理命令が読み出しの場合は、前記メモリデバイスからデータを受信するデータ受信手段と、前記メモリデバイスに送信するデータを記憶し、または、前記メモリデバイスから受信したデータを記憶するデータ記憶手段と、を備えることを特徴とする情報機器。

14. 前記検証情報生成手段の前記検証情報の生成処理が、前記指定情報と検証用鍵とを用いて行うことを特徴とする請求の範囲13記載の情報機器。

15. 前記メモリデバイスとの間で前記検証用鍵を共有する検証用鍵共有手段を備えることを特徴とする請求の範囲14記載の情報機器。

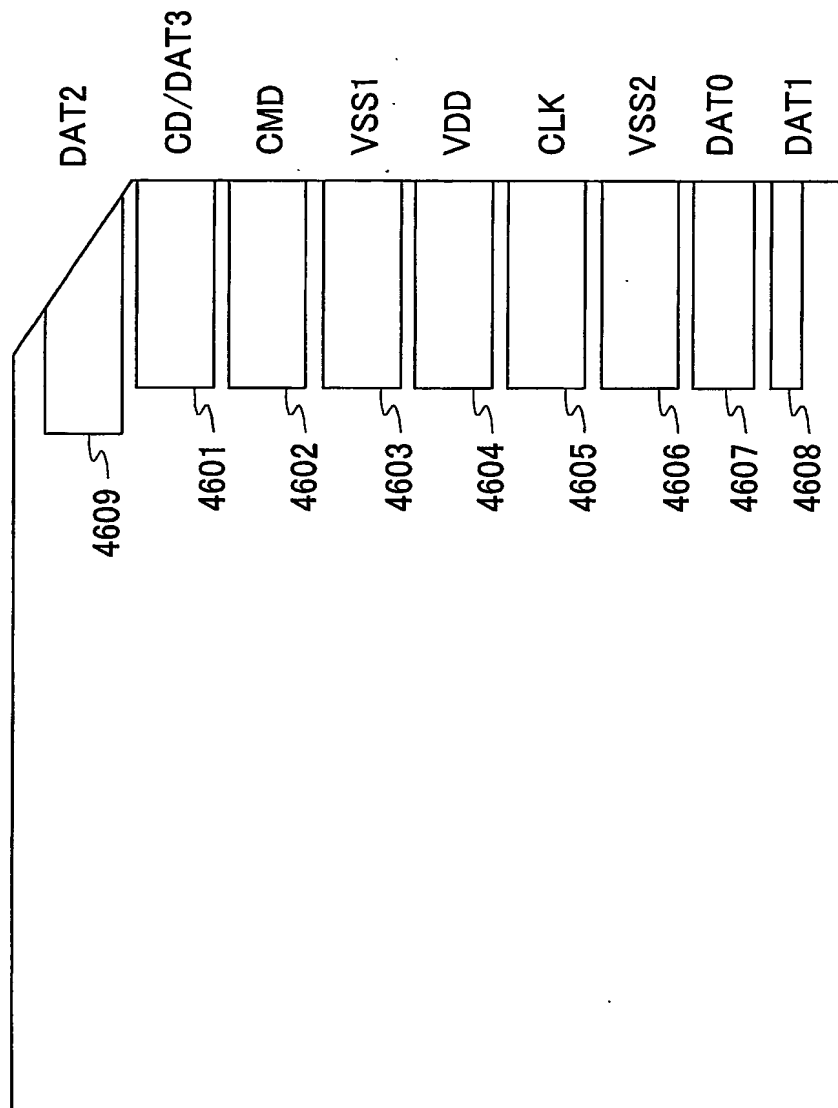
16. 前記メモリデバイスとの間で、当該メモリデバイスへのアクセス可能な領域を示す可能領域情報を共有する可能領域情報共有手段をさらに備えることを特徴とする請求の範囲13記載の情報機器。

17. 機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと検証用鍵とを用いて検証するステップと、前記検証に成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

18. 機器からメモリデバイスに対するアクセス方法であって、前記機器は、第一の処理系コマンドを用いて前記メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて前記アクセス可能領域に対応した検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて前記アクセス領域

への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合は、前記処理命令を実行するステップと、を有するアクセス方法。

19. 機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性かつ大容量の第2領域と、前記機器からアクセスすることが可能かつ大容量の第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。



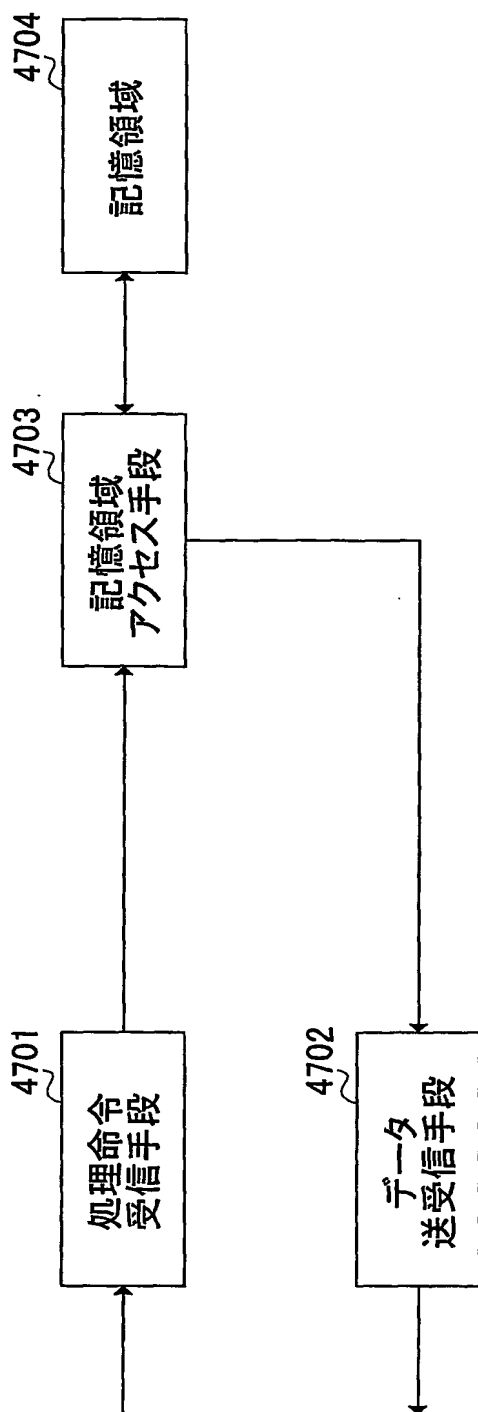


図2

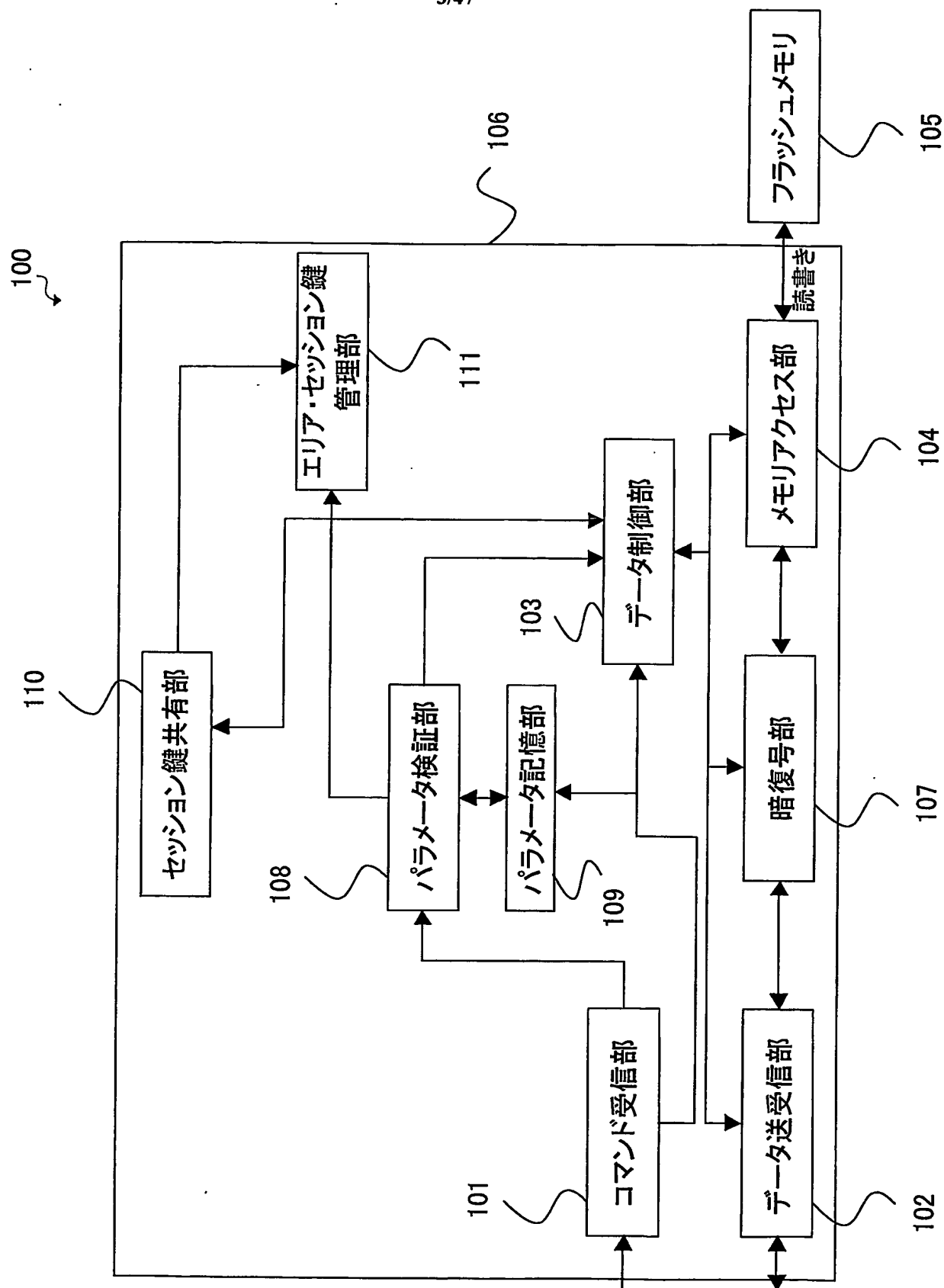
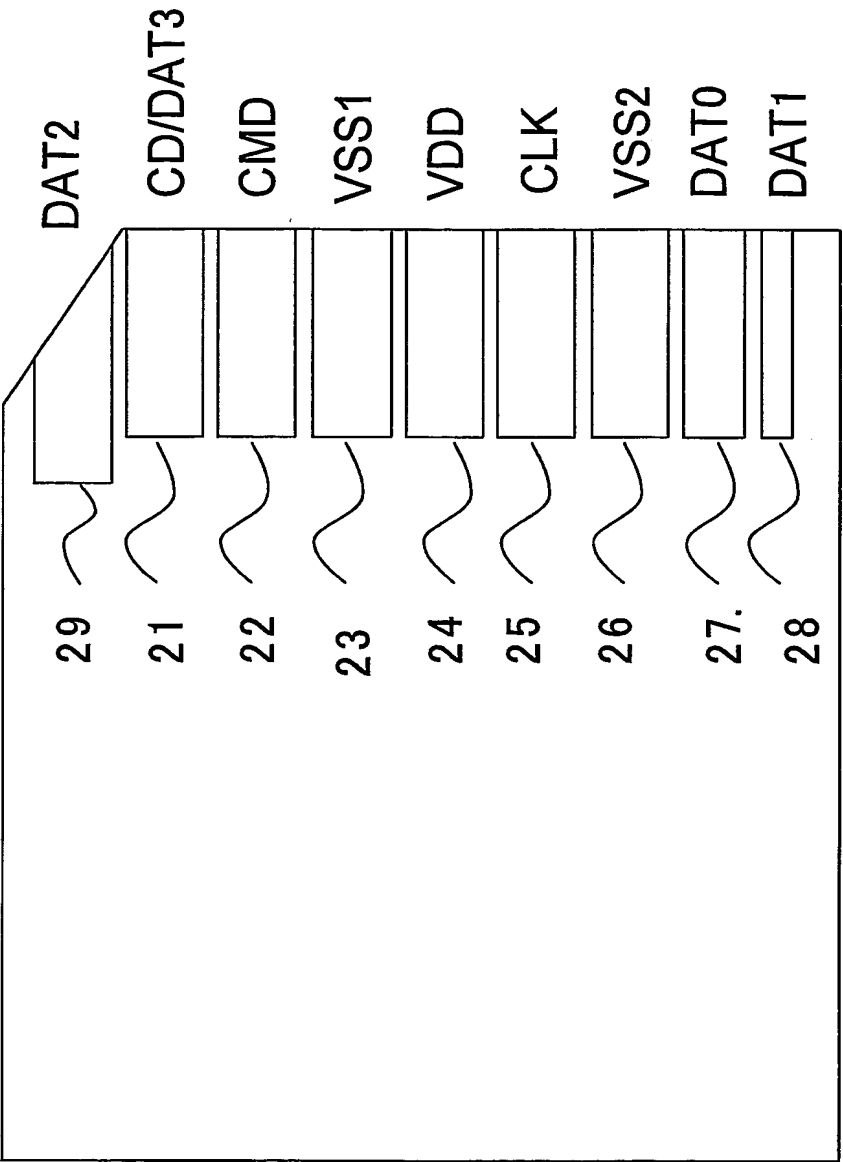


図3



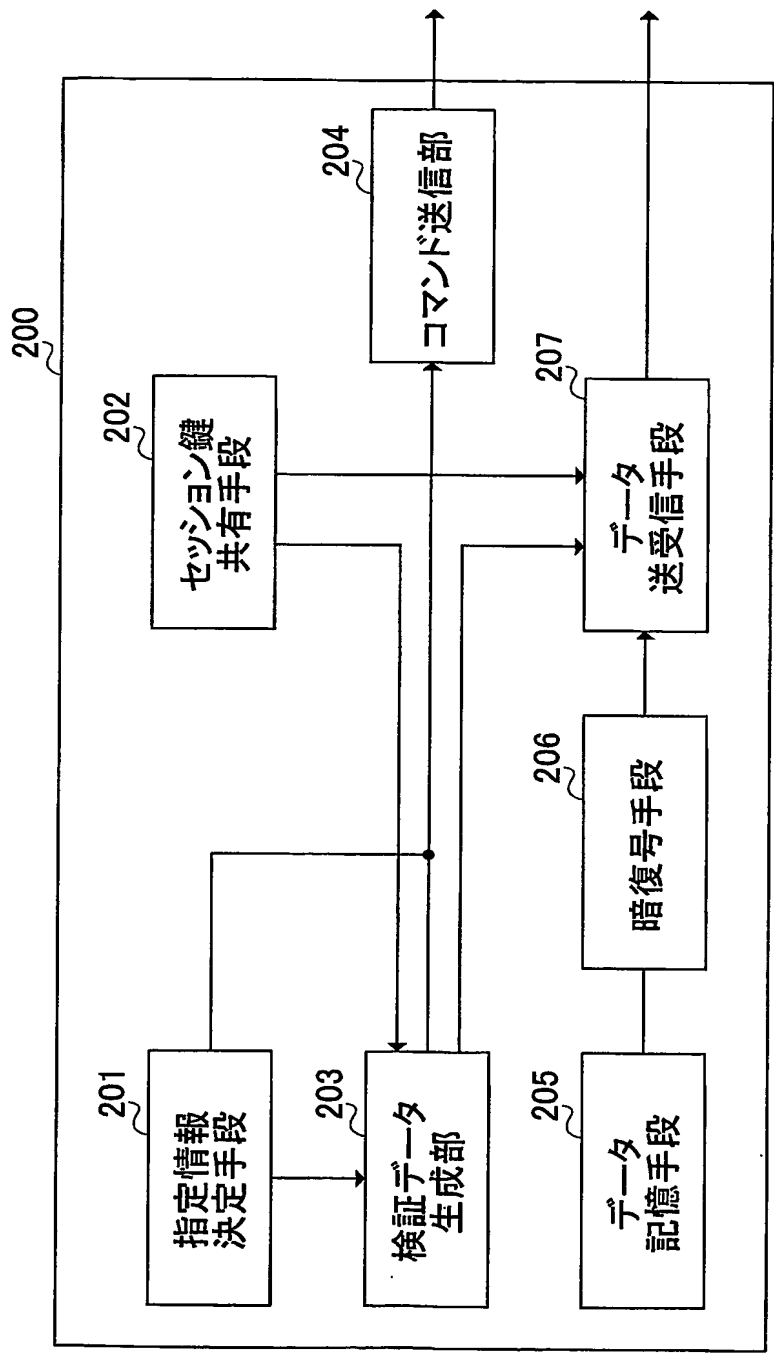


図5

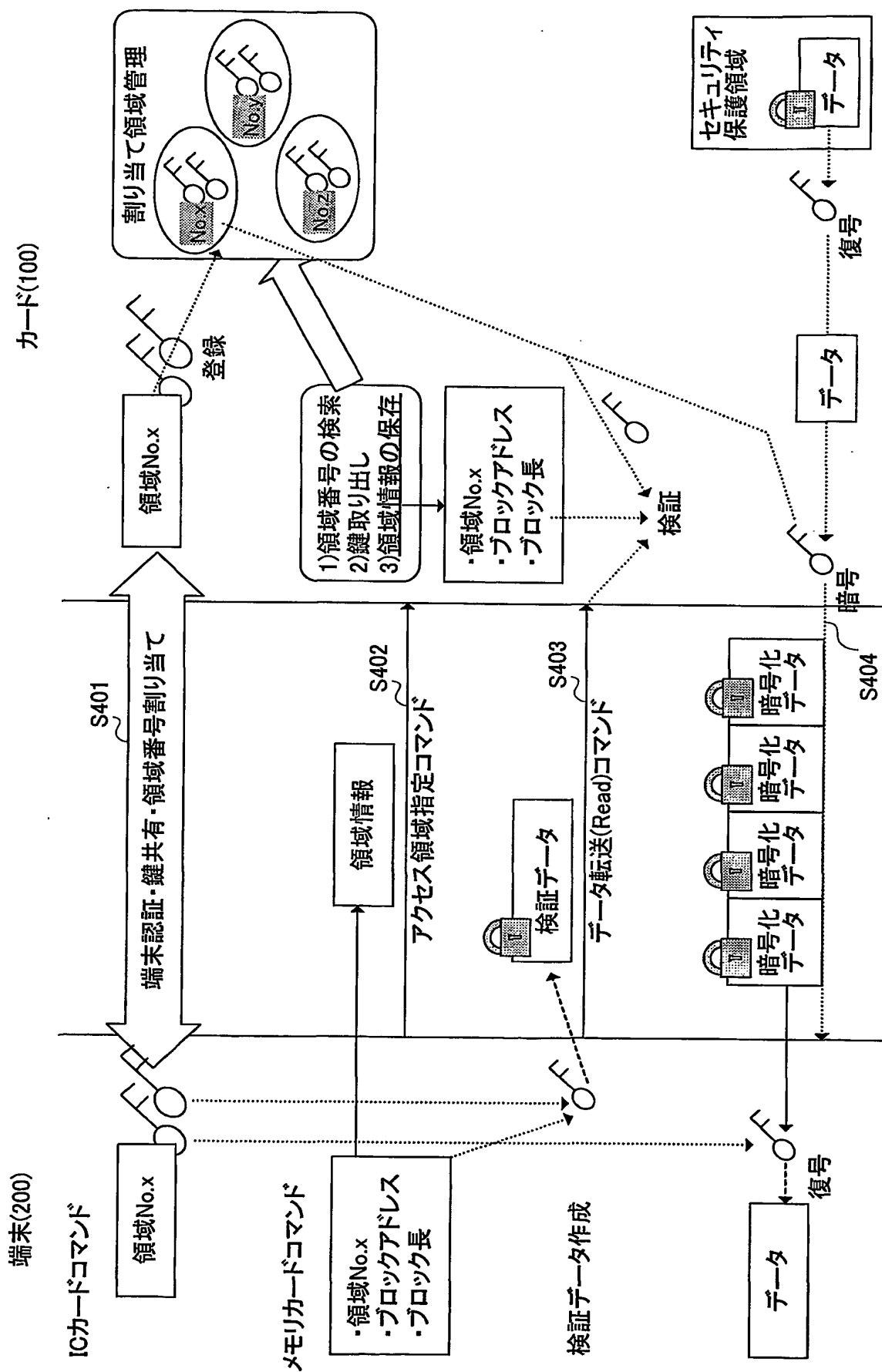


図 9

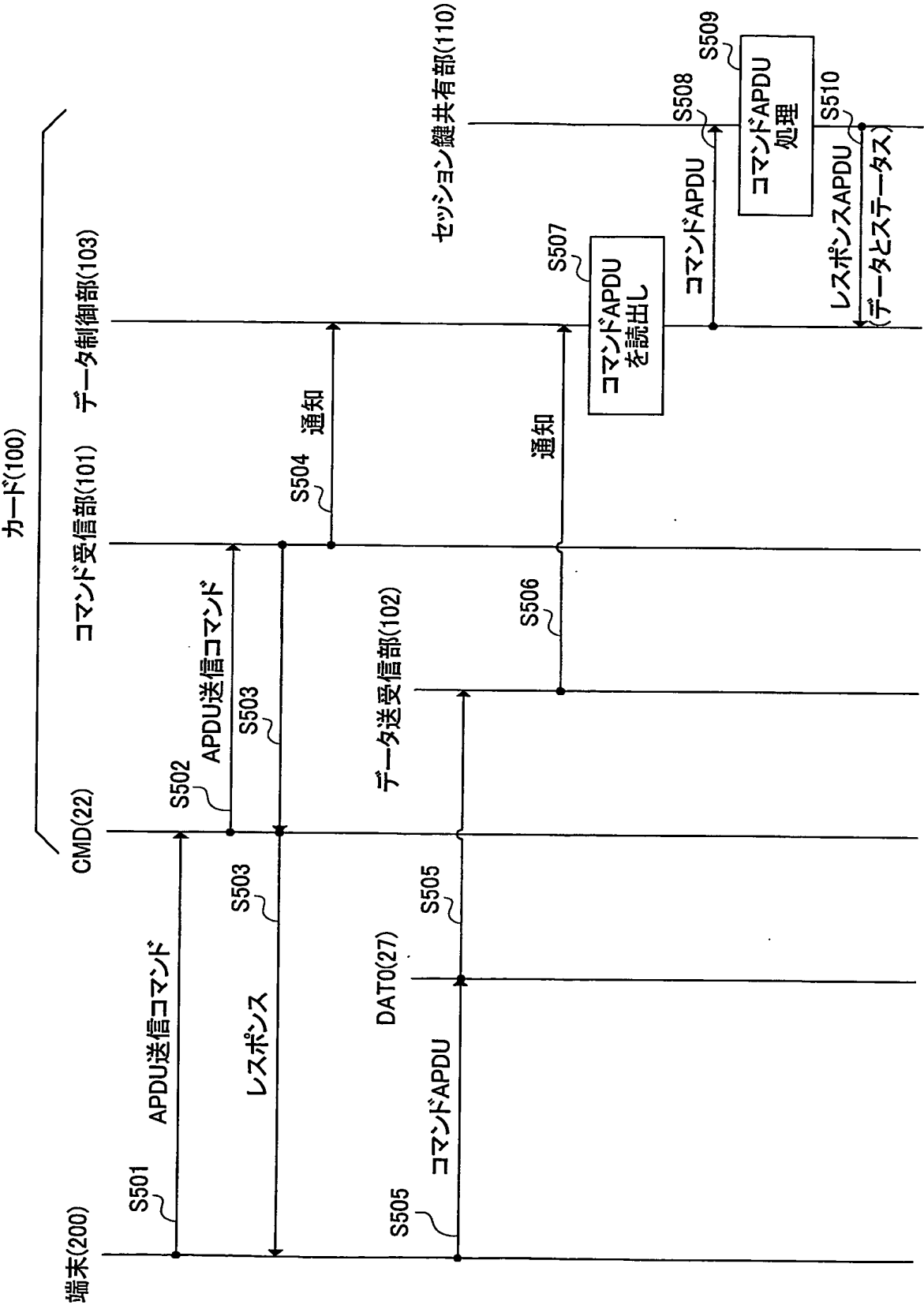


図7

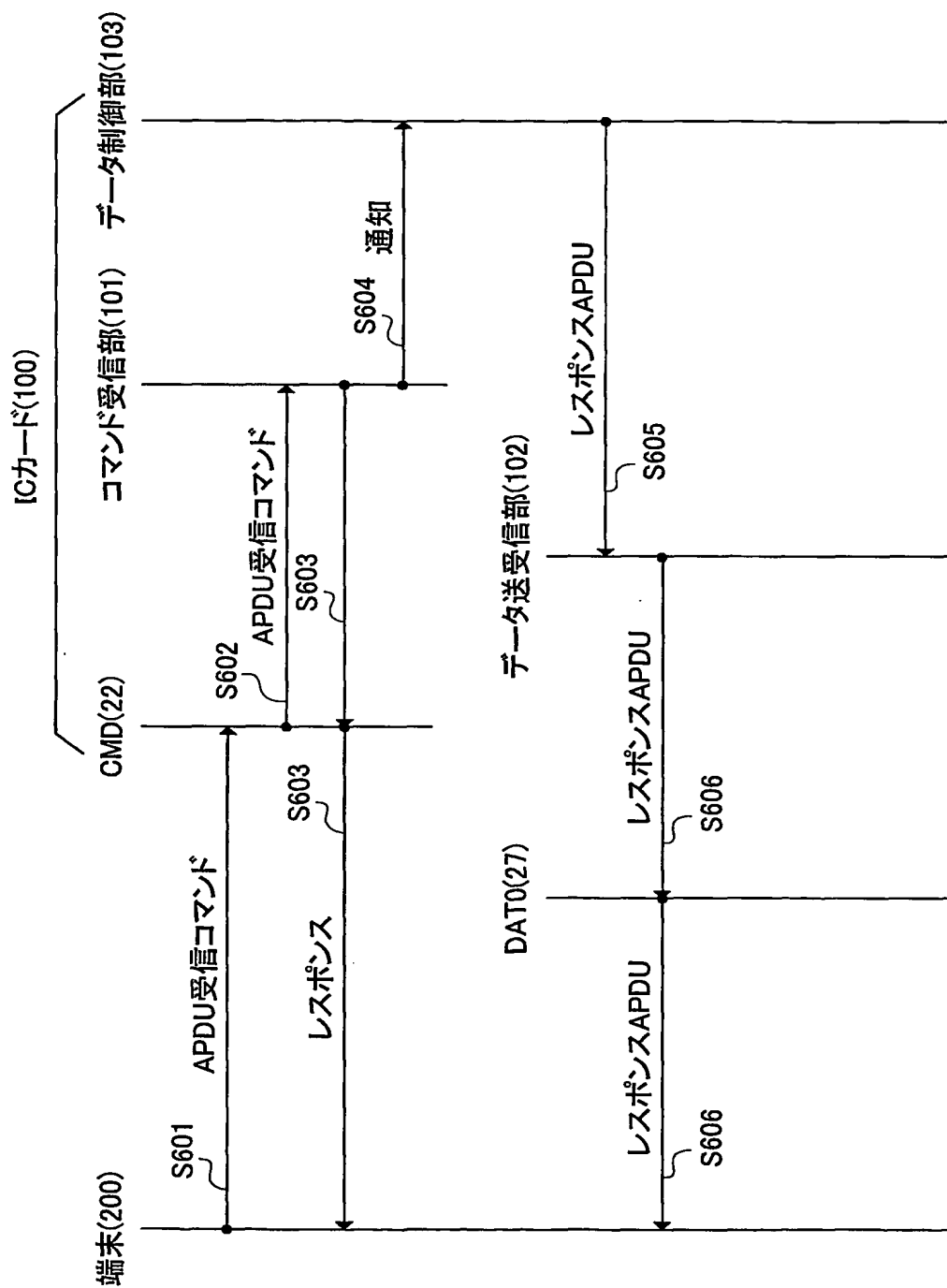
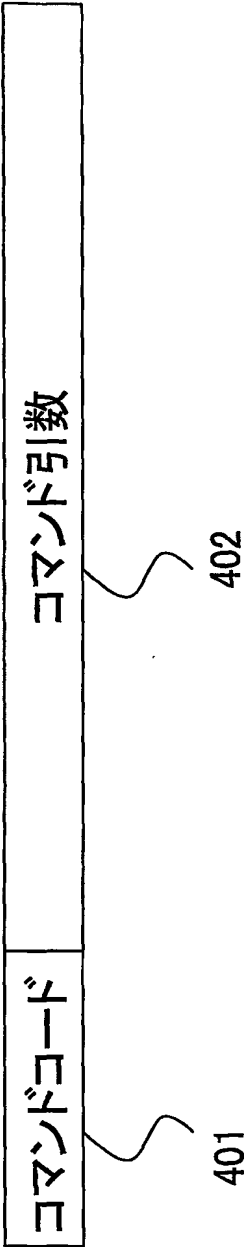


図8



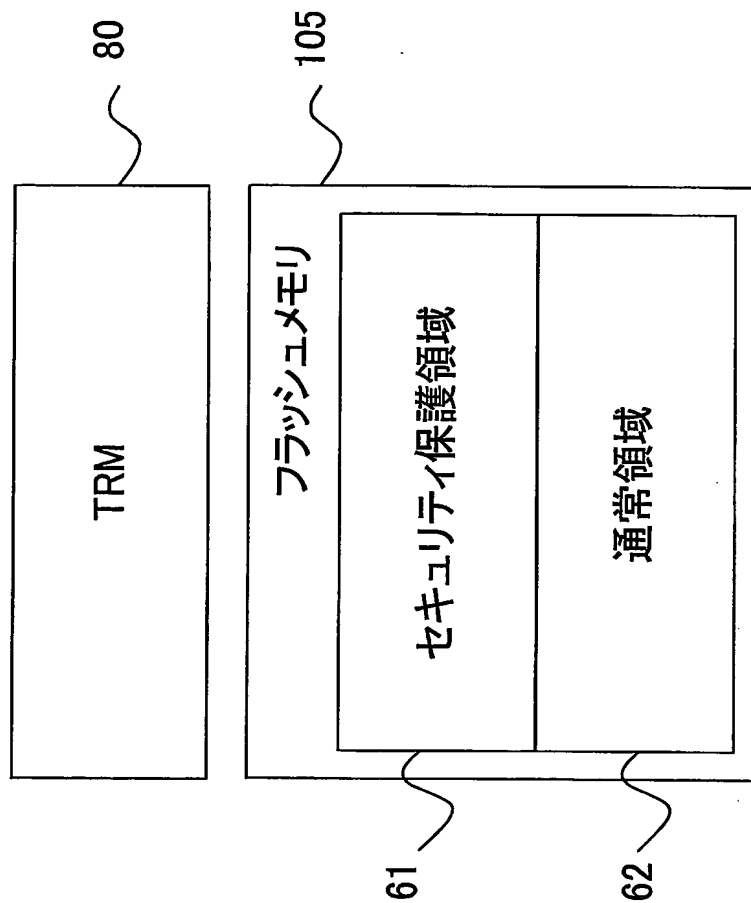


図10

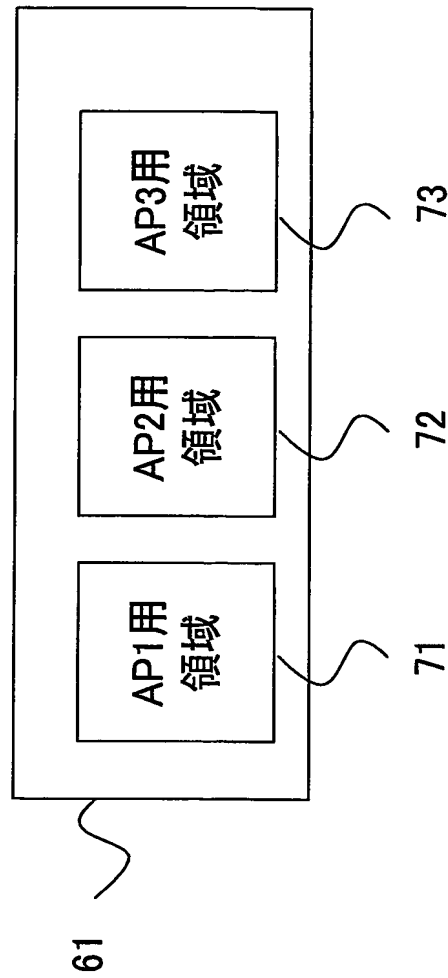


図11

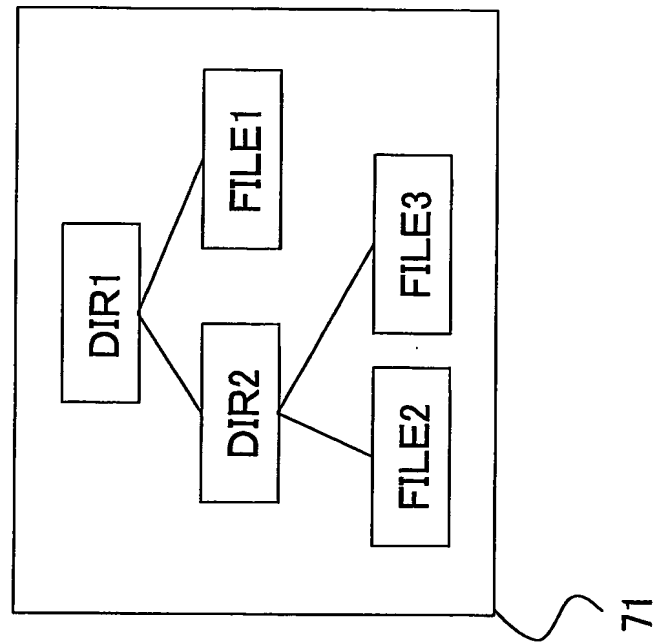


図12

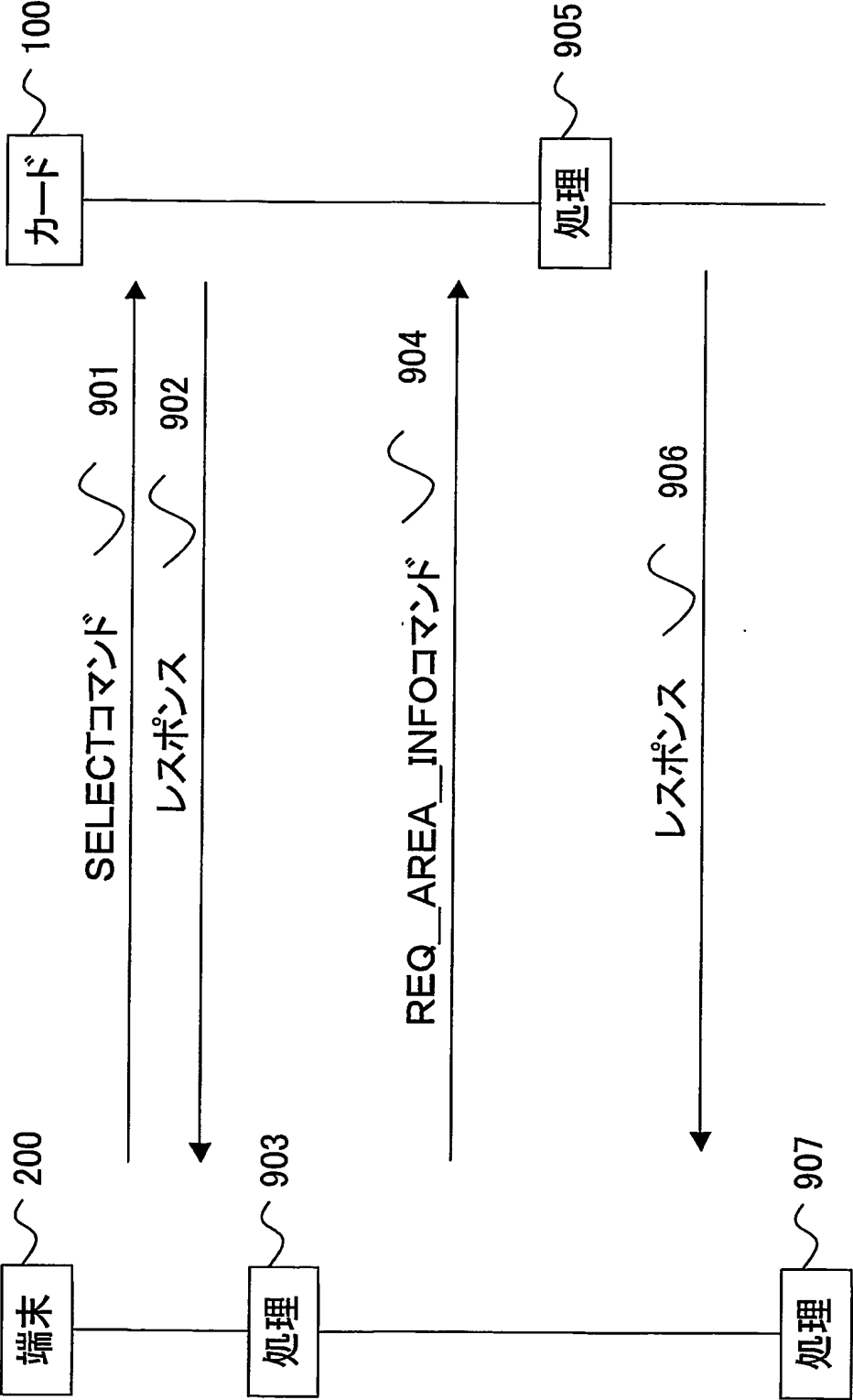


図13

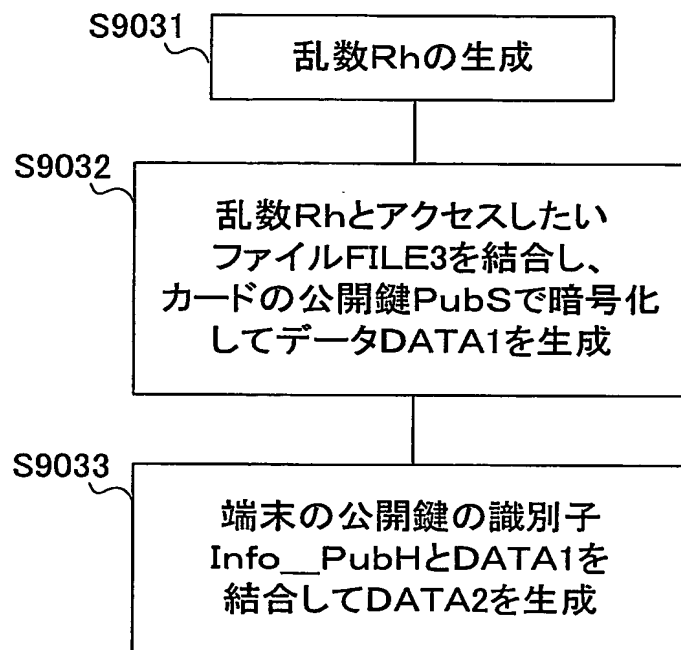


図14

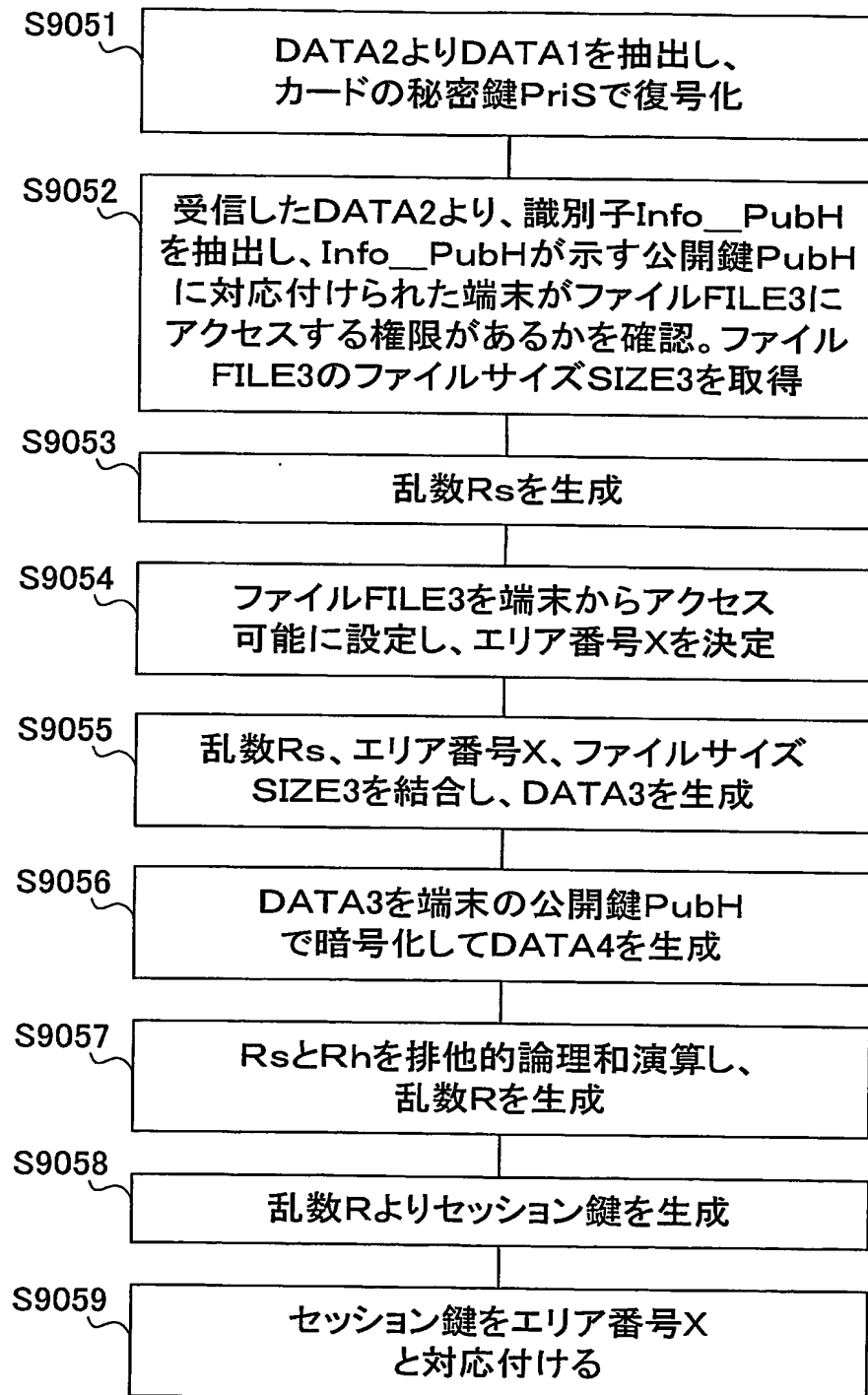


図15

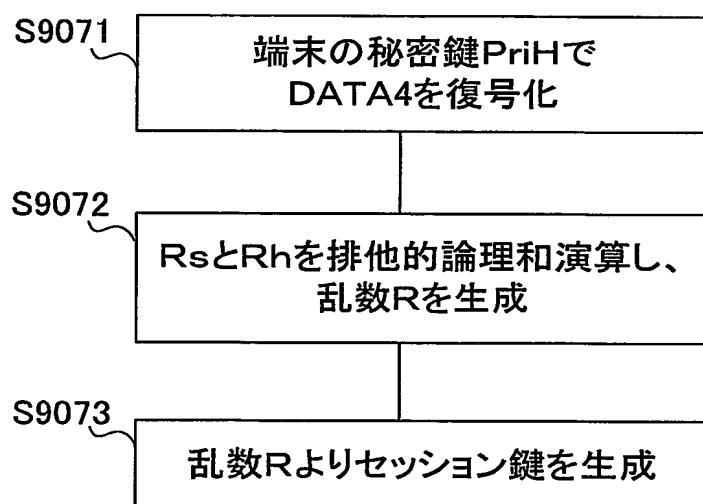


図16

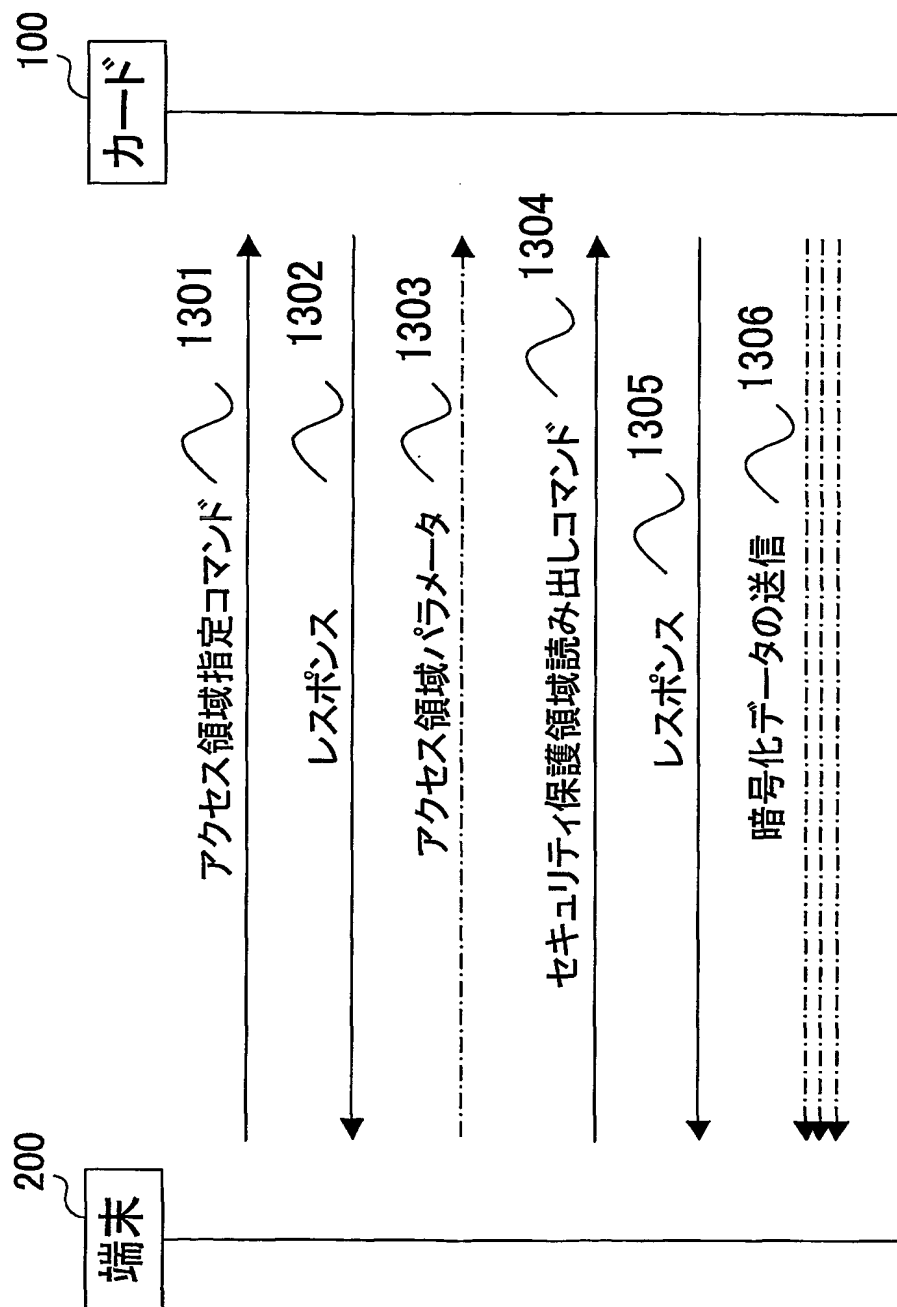


図17

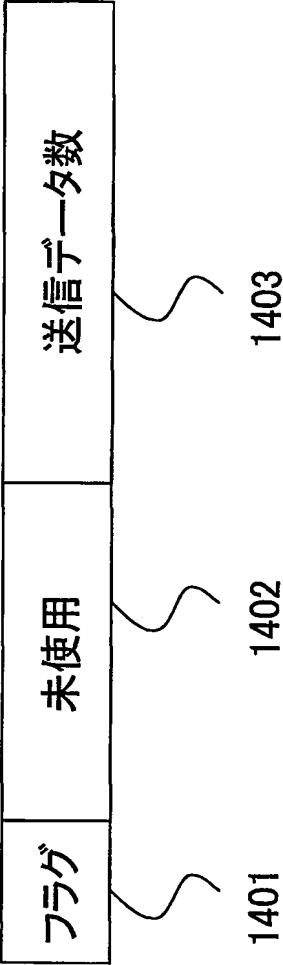


図18

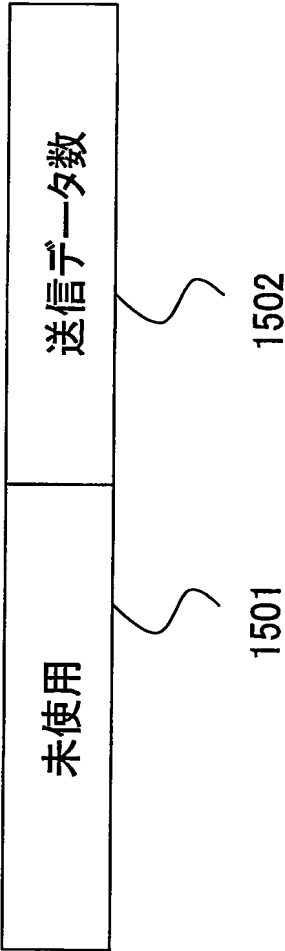


図19

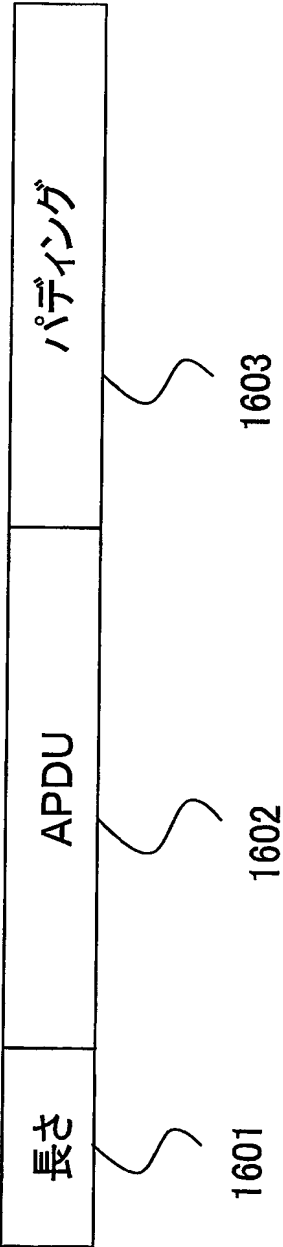


図20

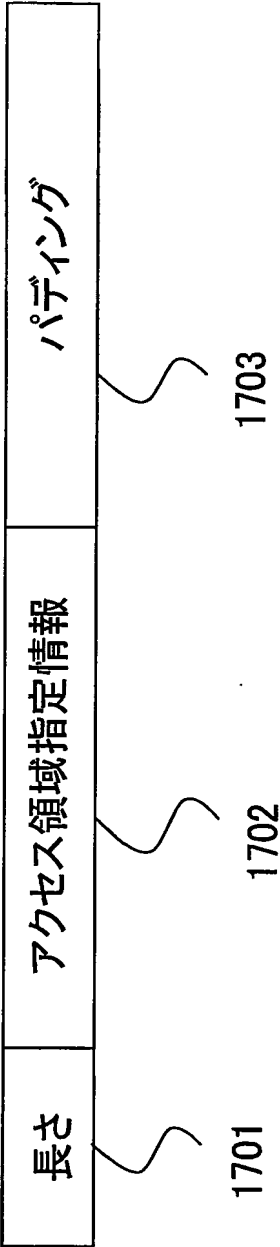


図21

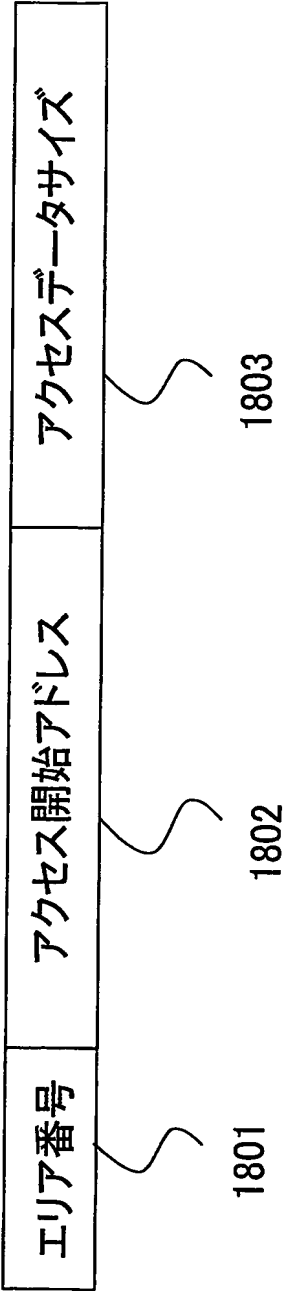


図22

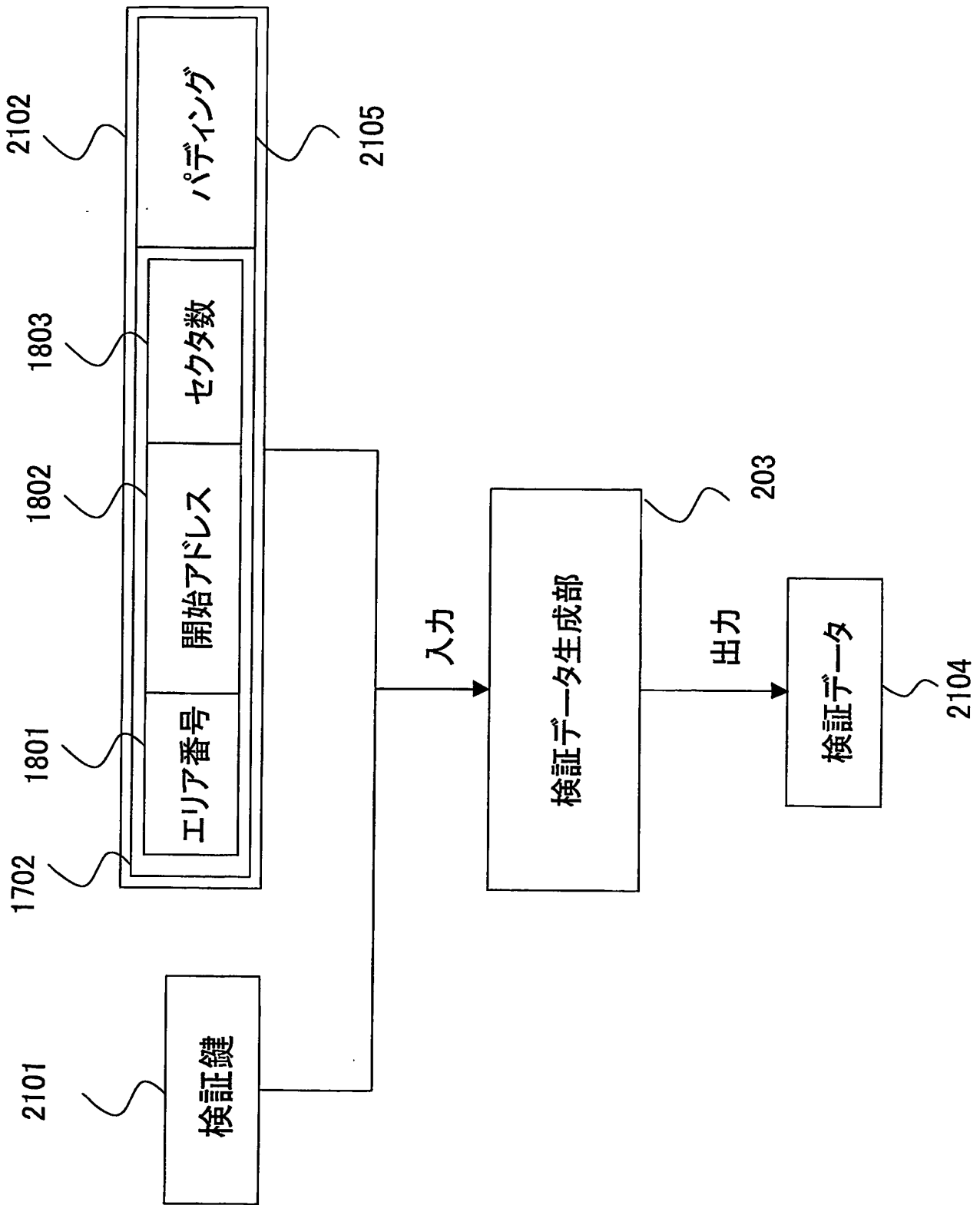


図23

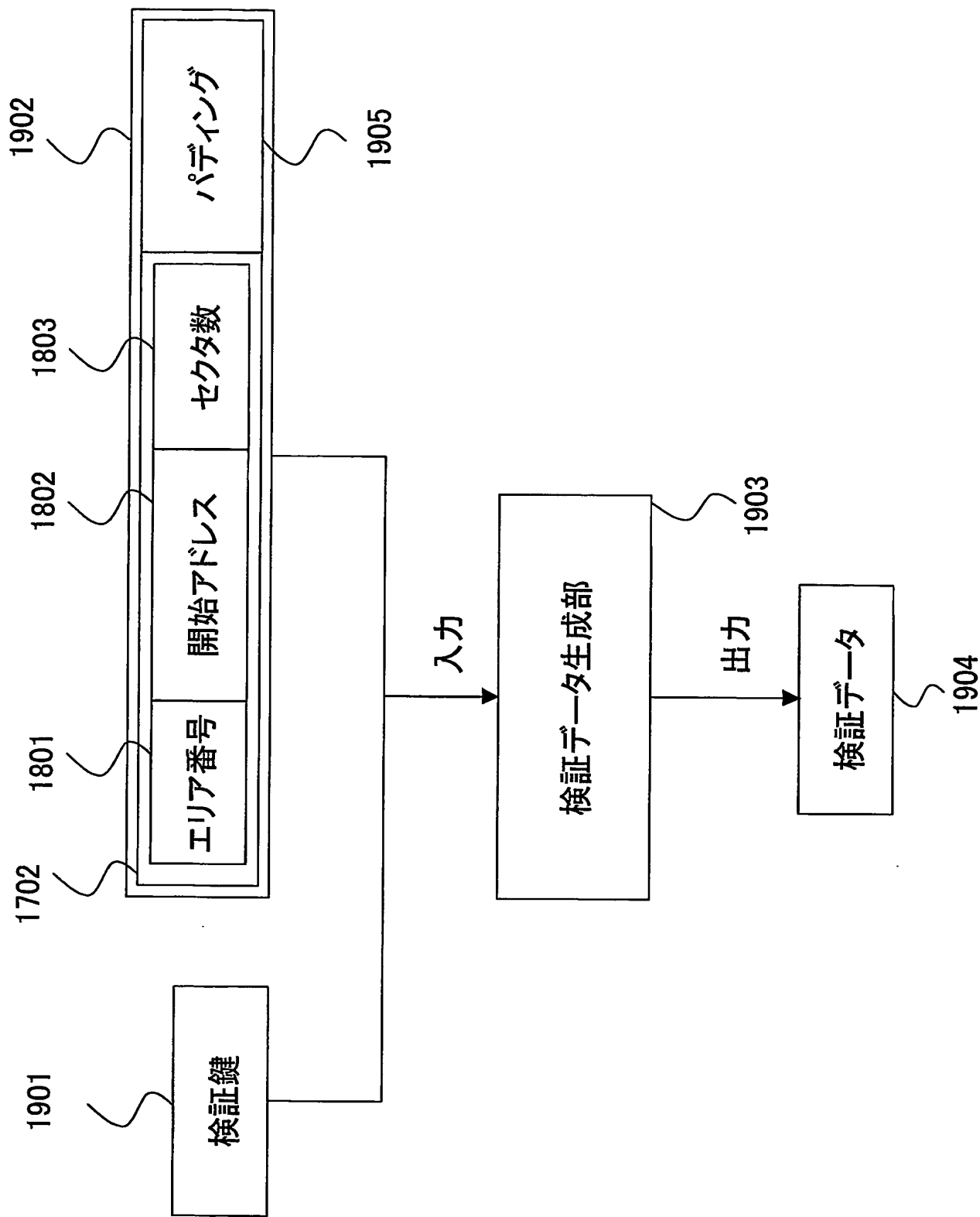


図24

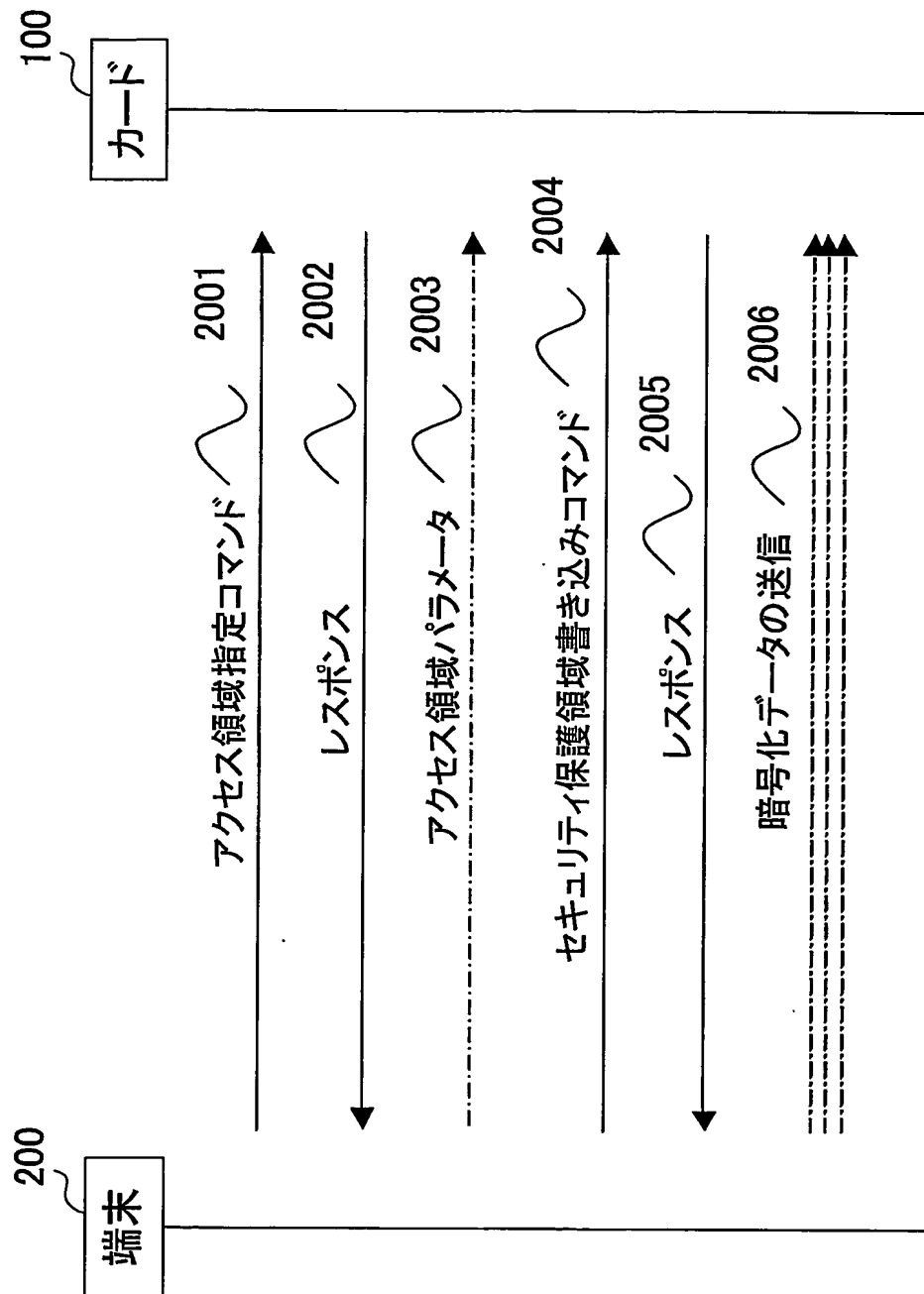


図25

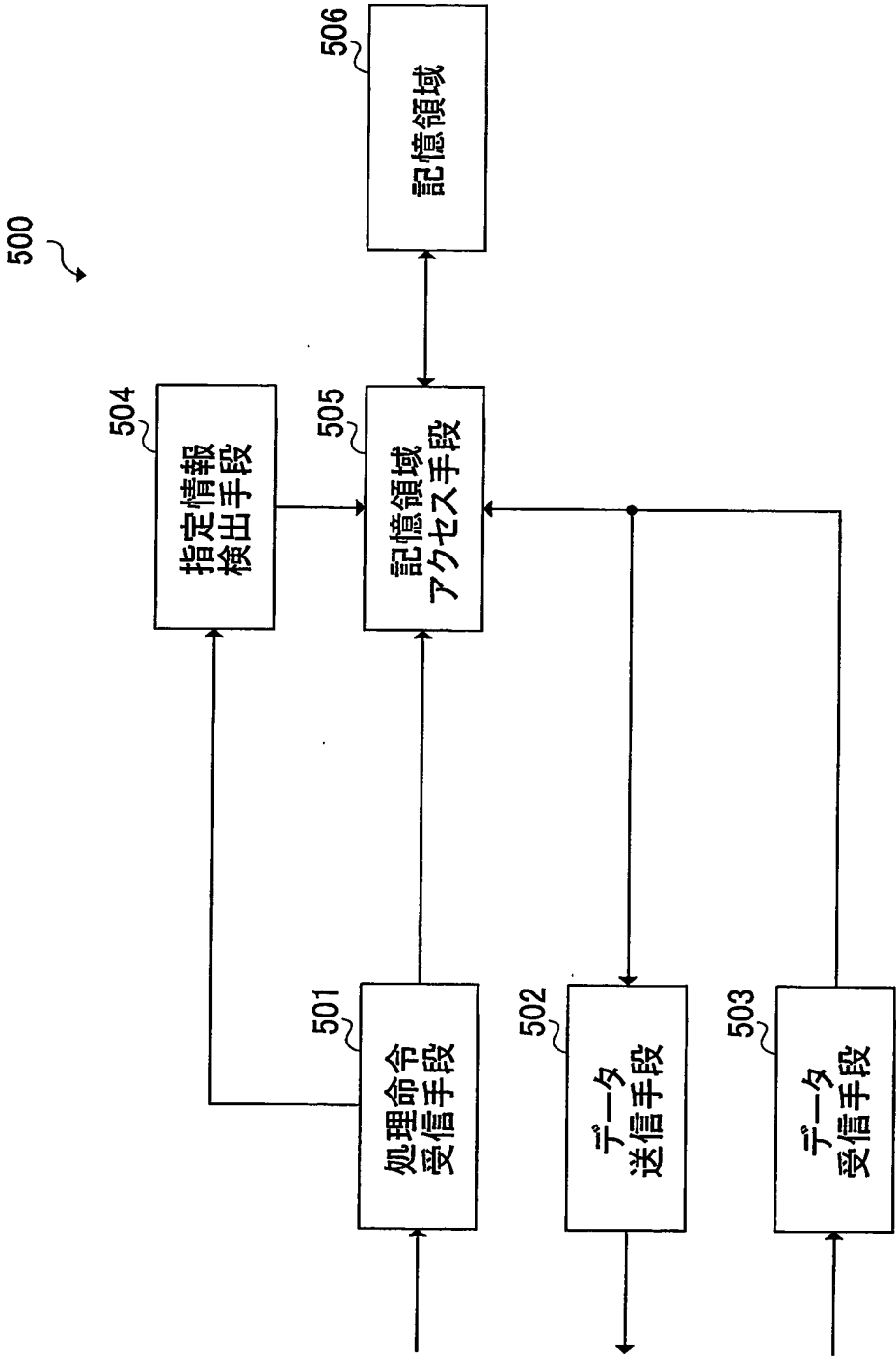


図26

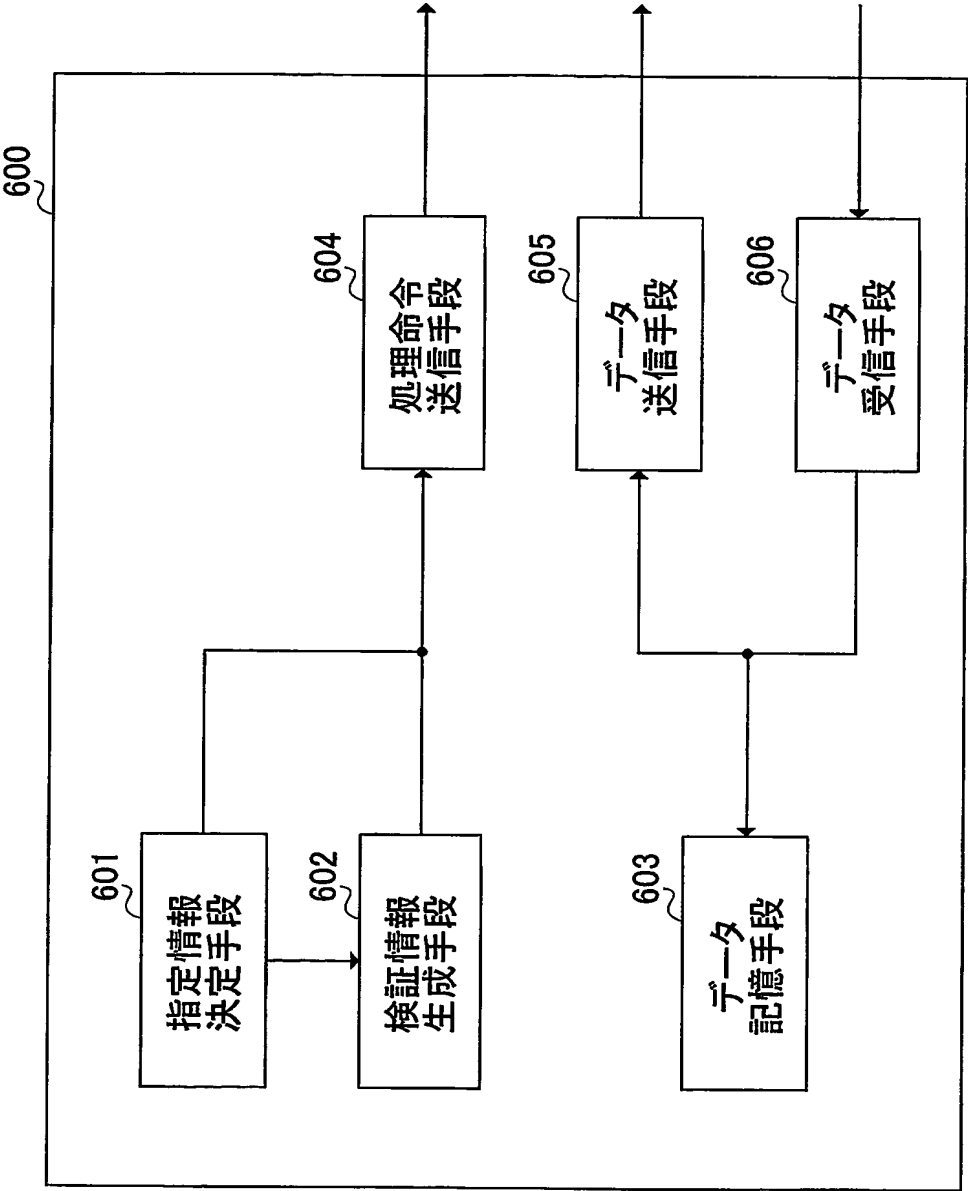


図27

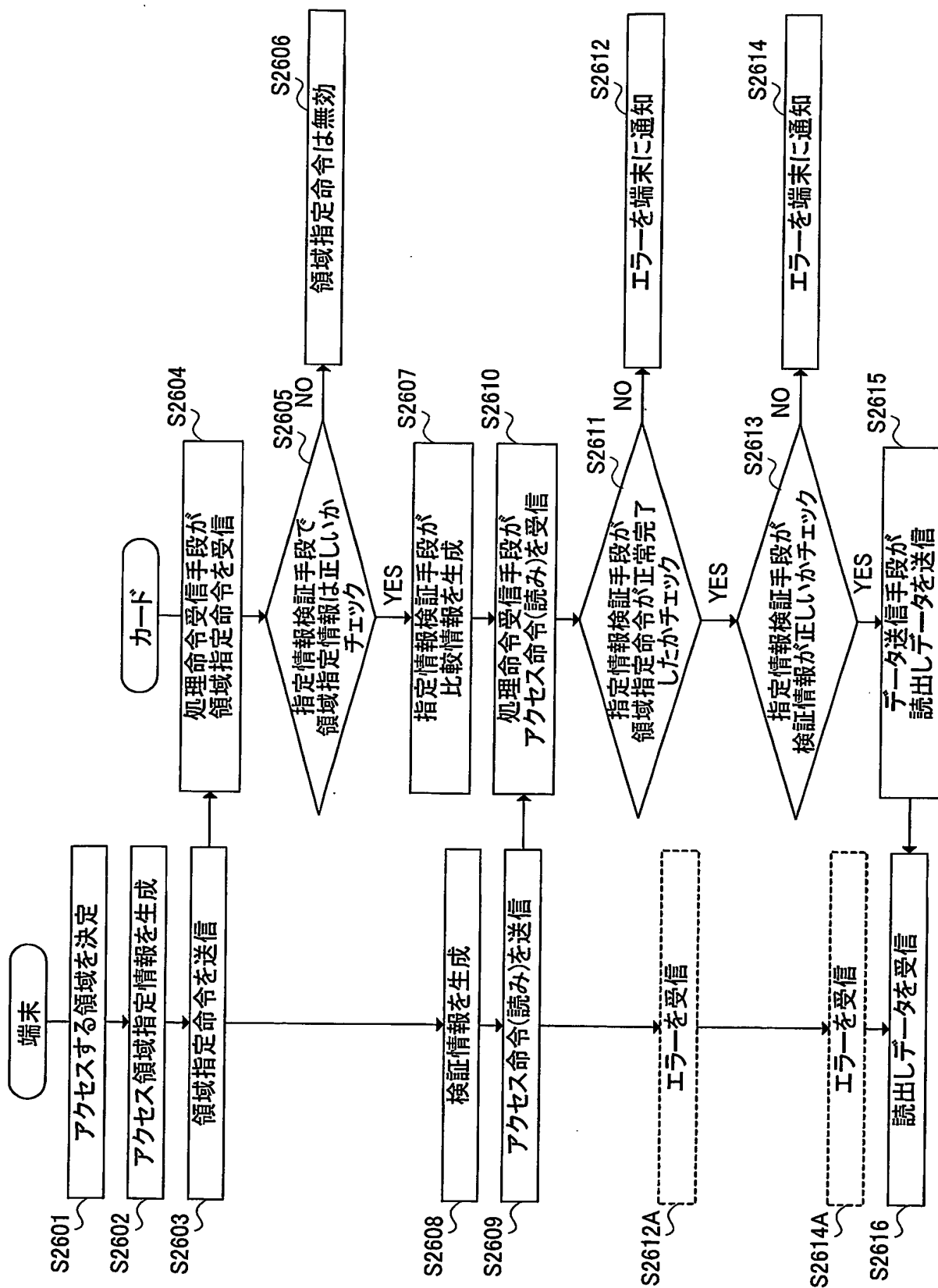


図28

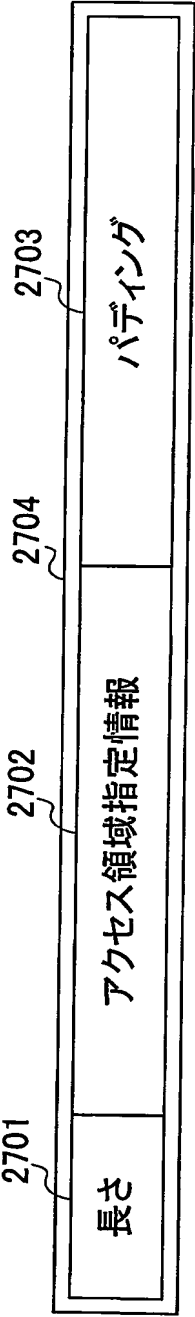
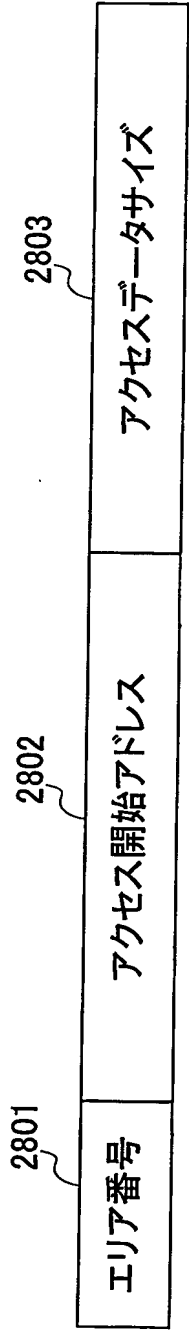


図29



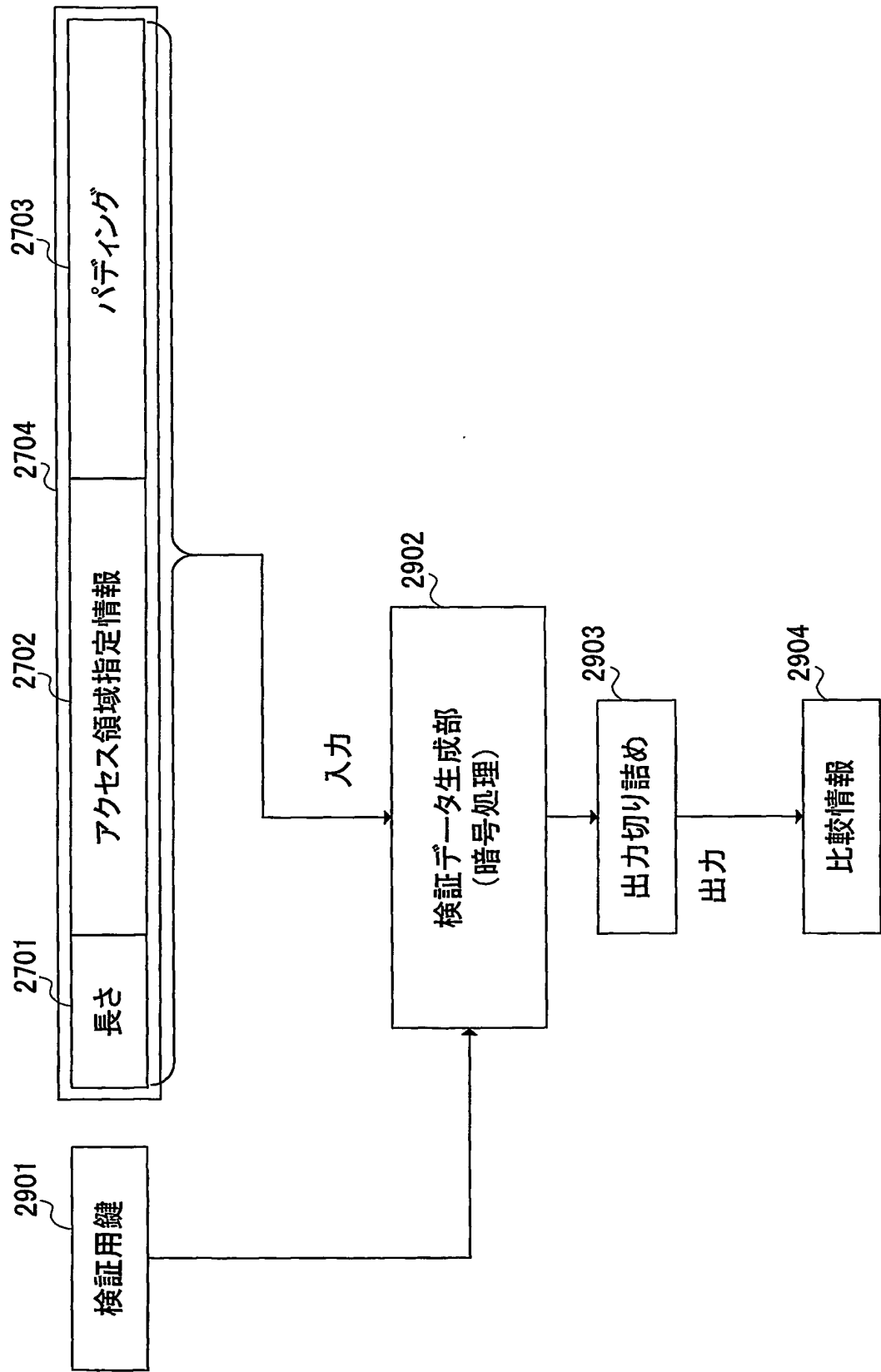


図31

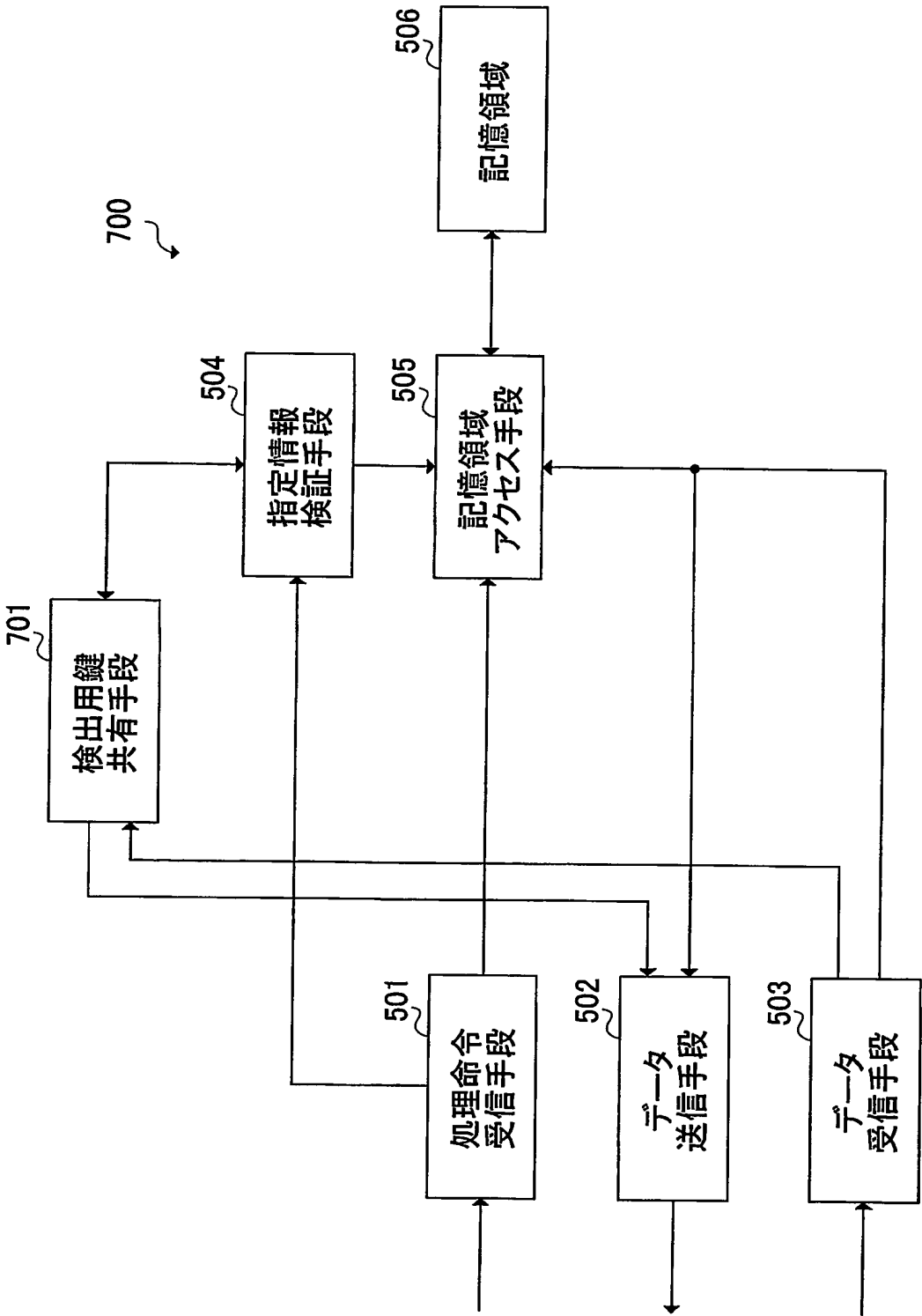


図32

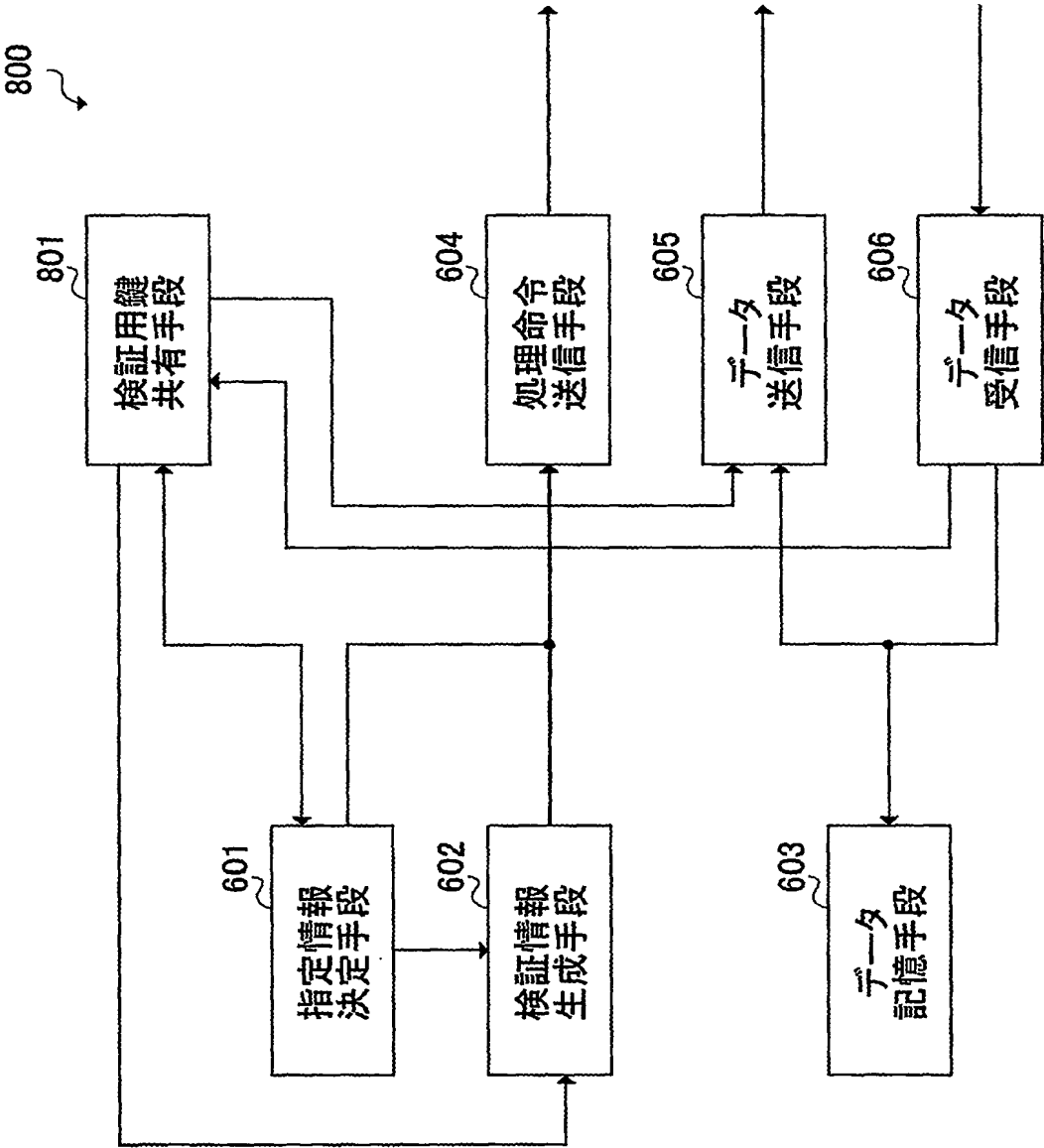


図33

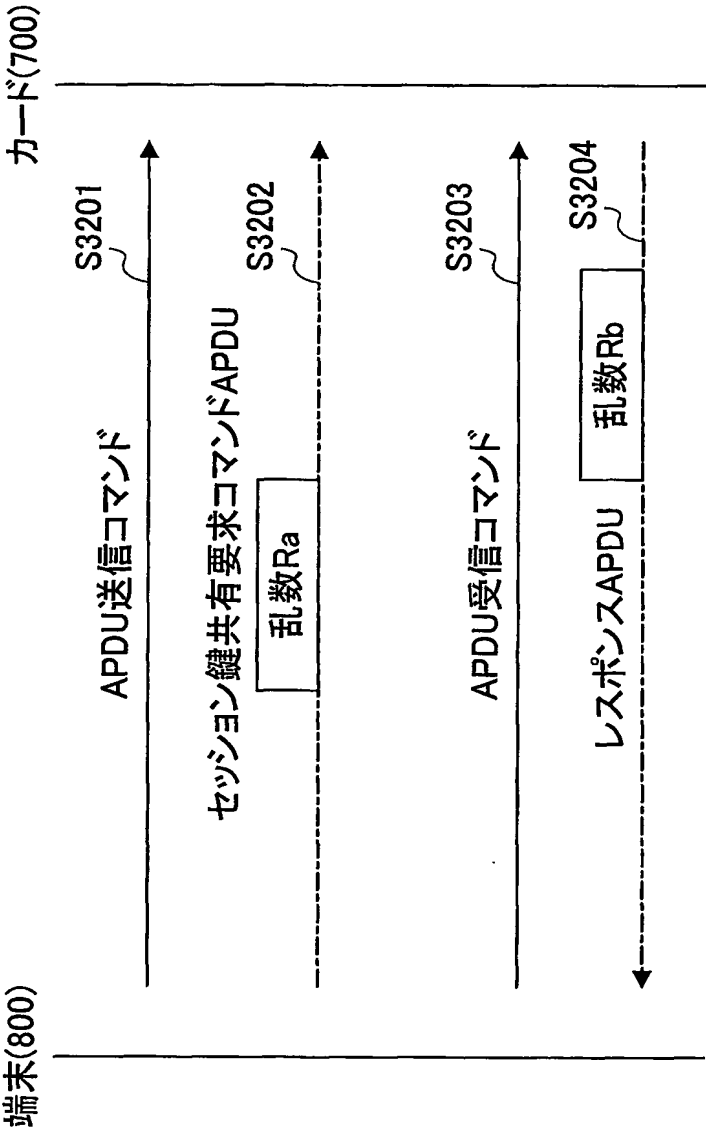


図 34

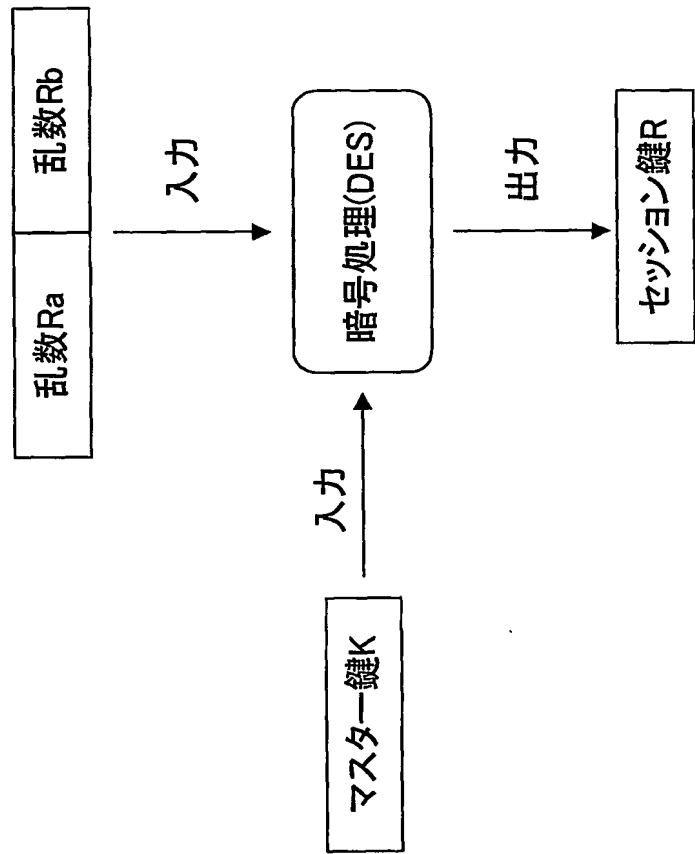


図35

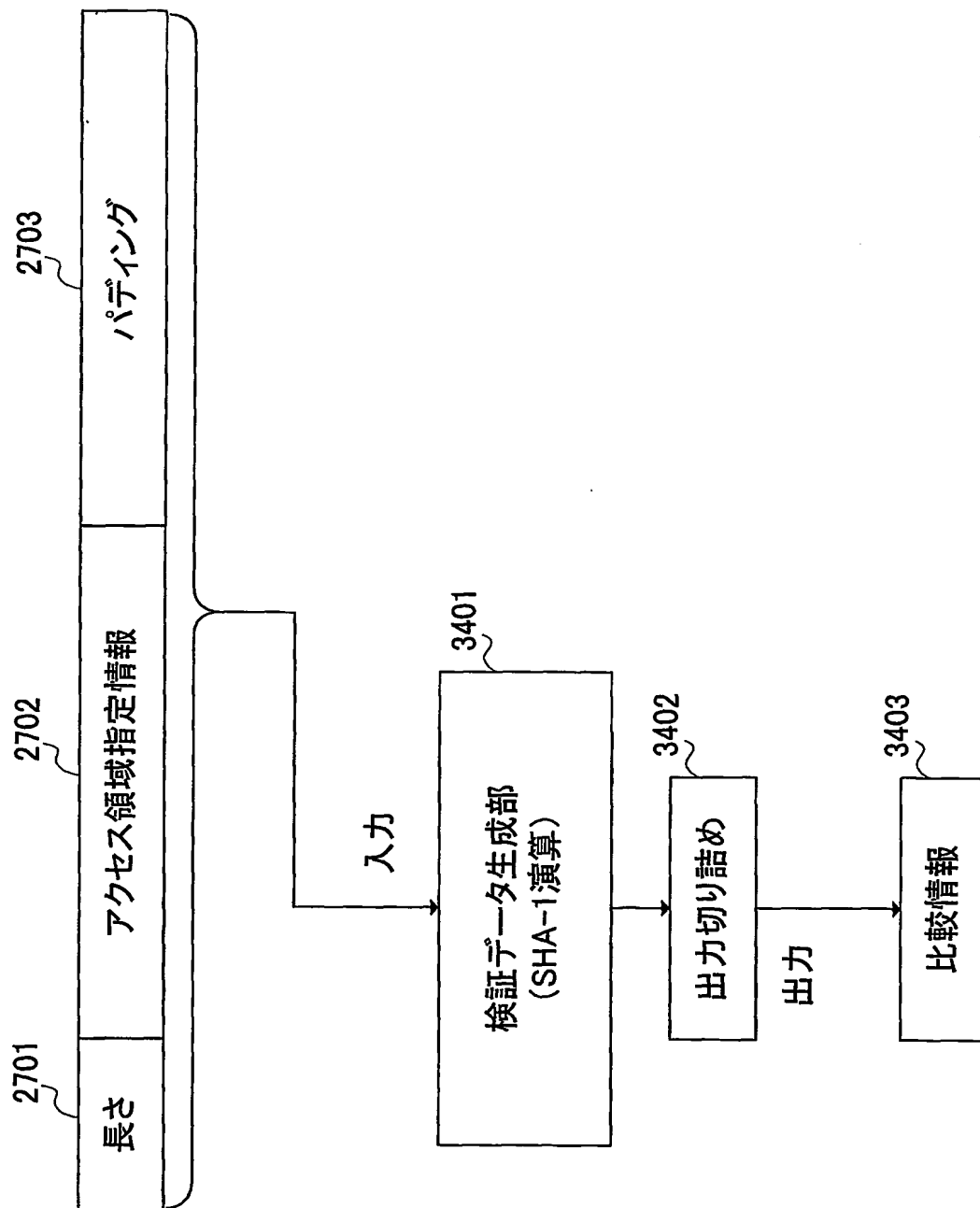


図36

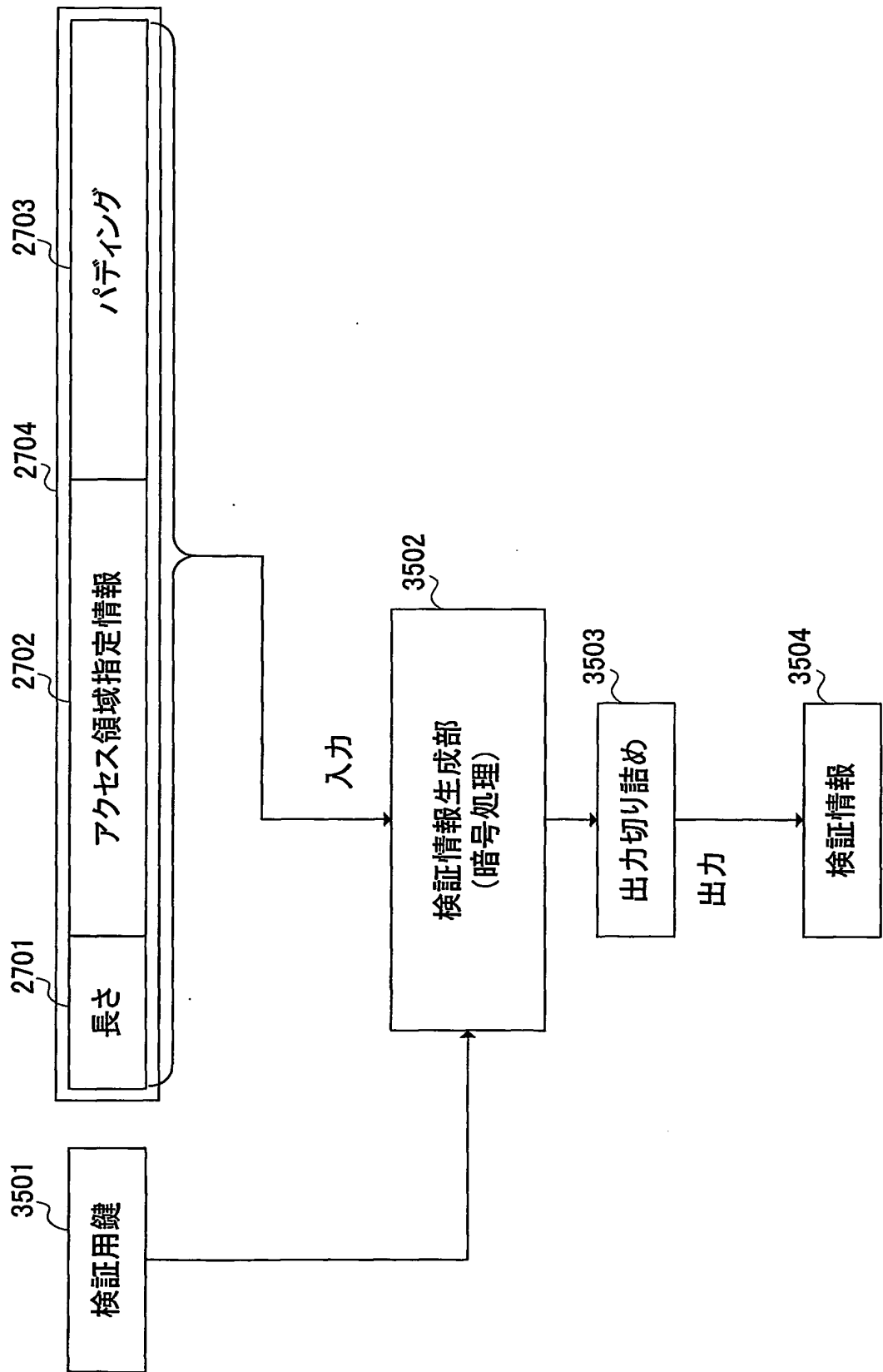


図37

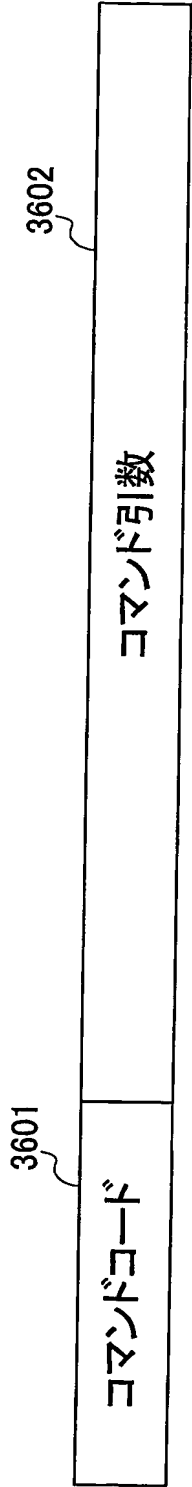


図 38

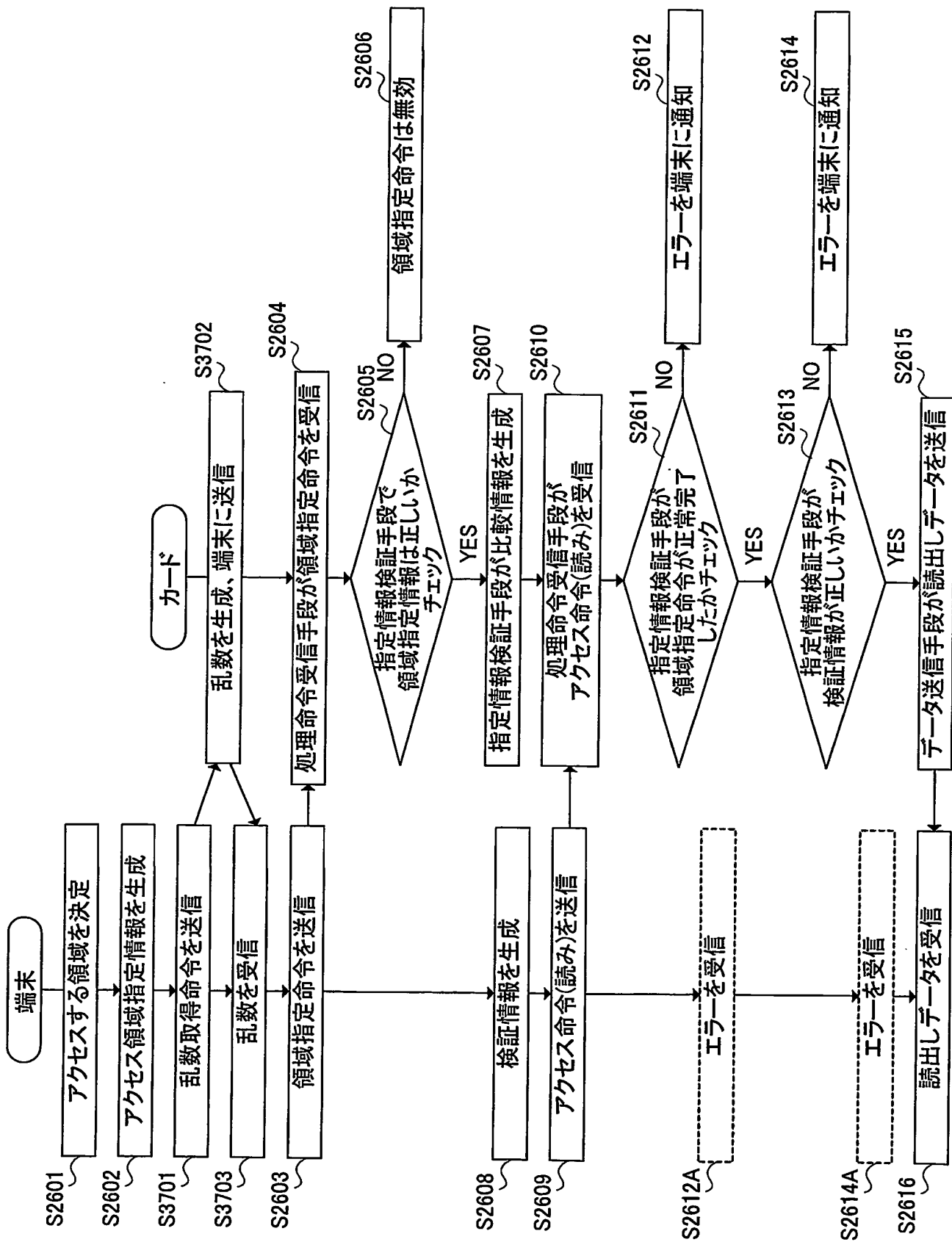


図39

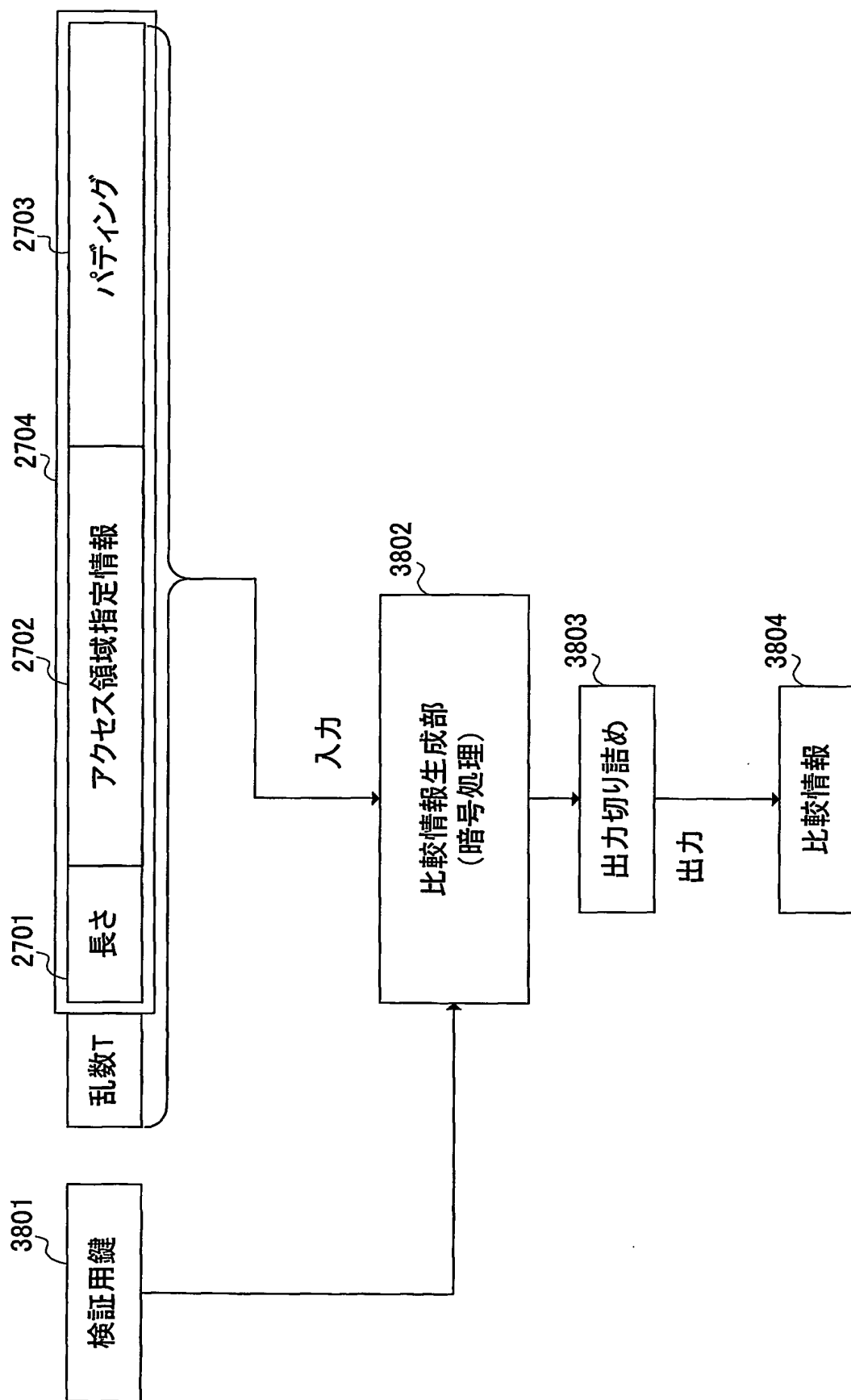


図40

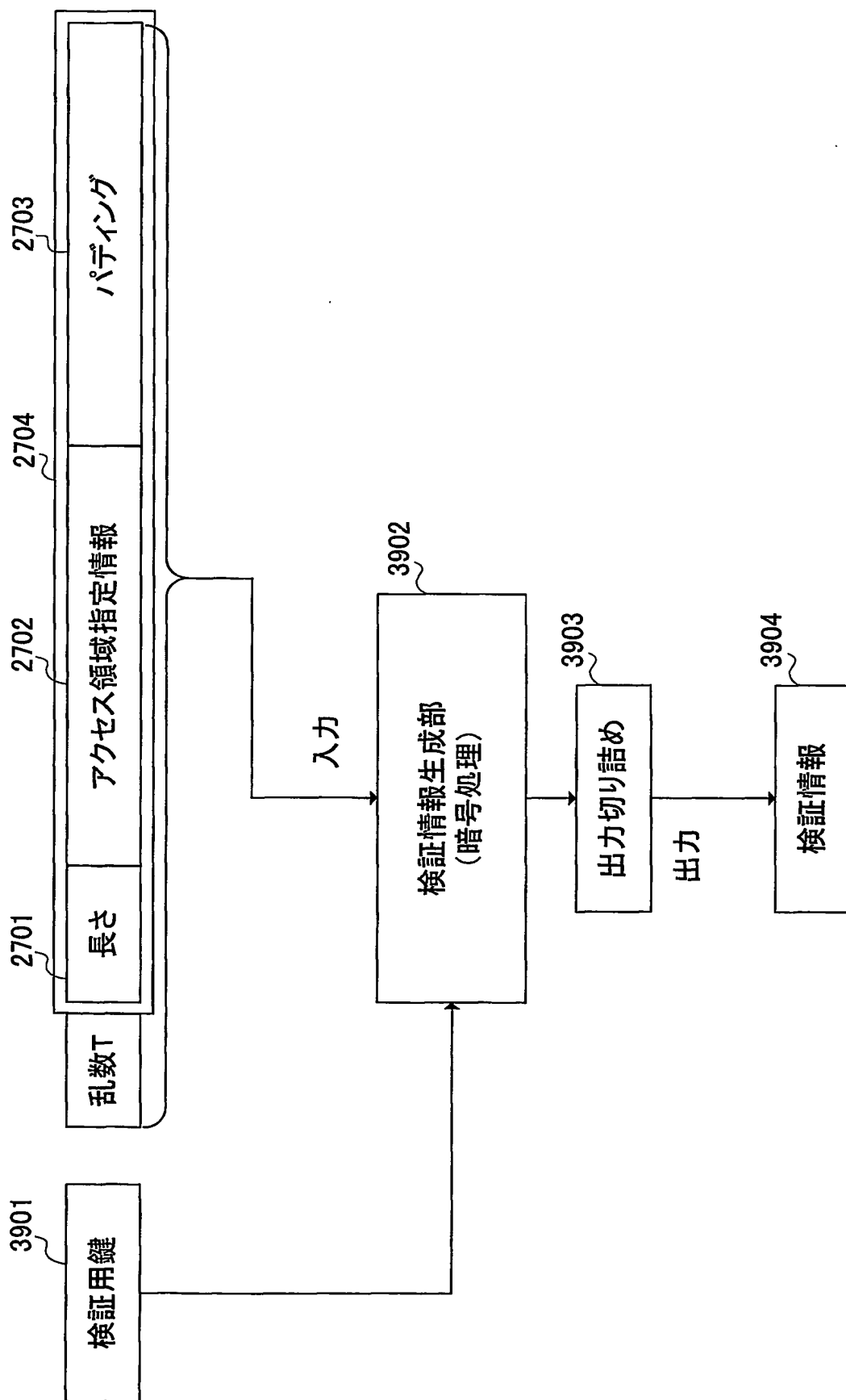


図41

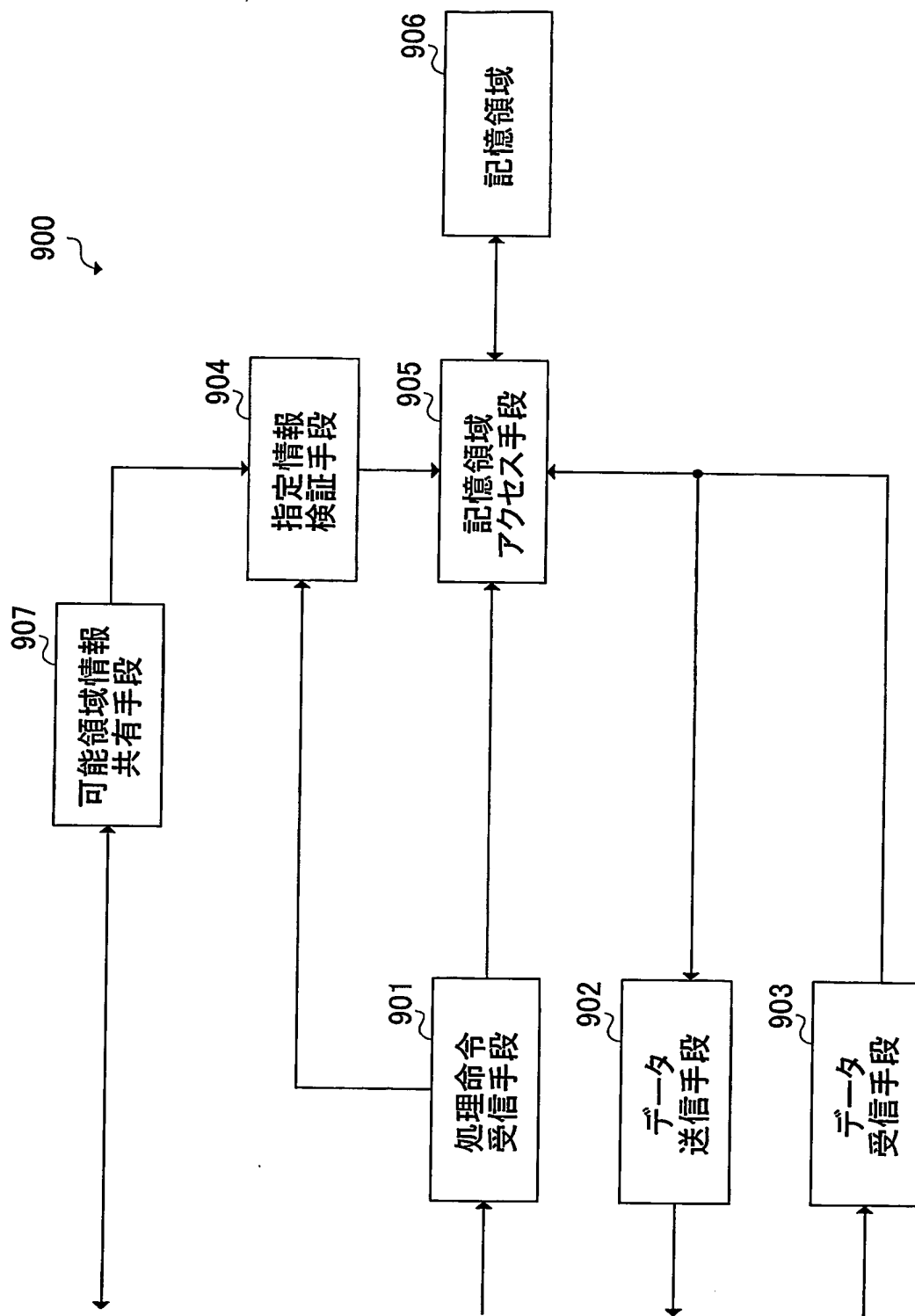


図42

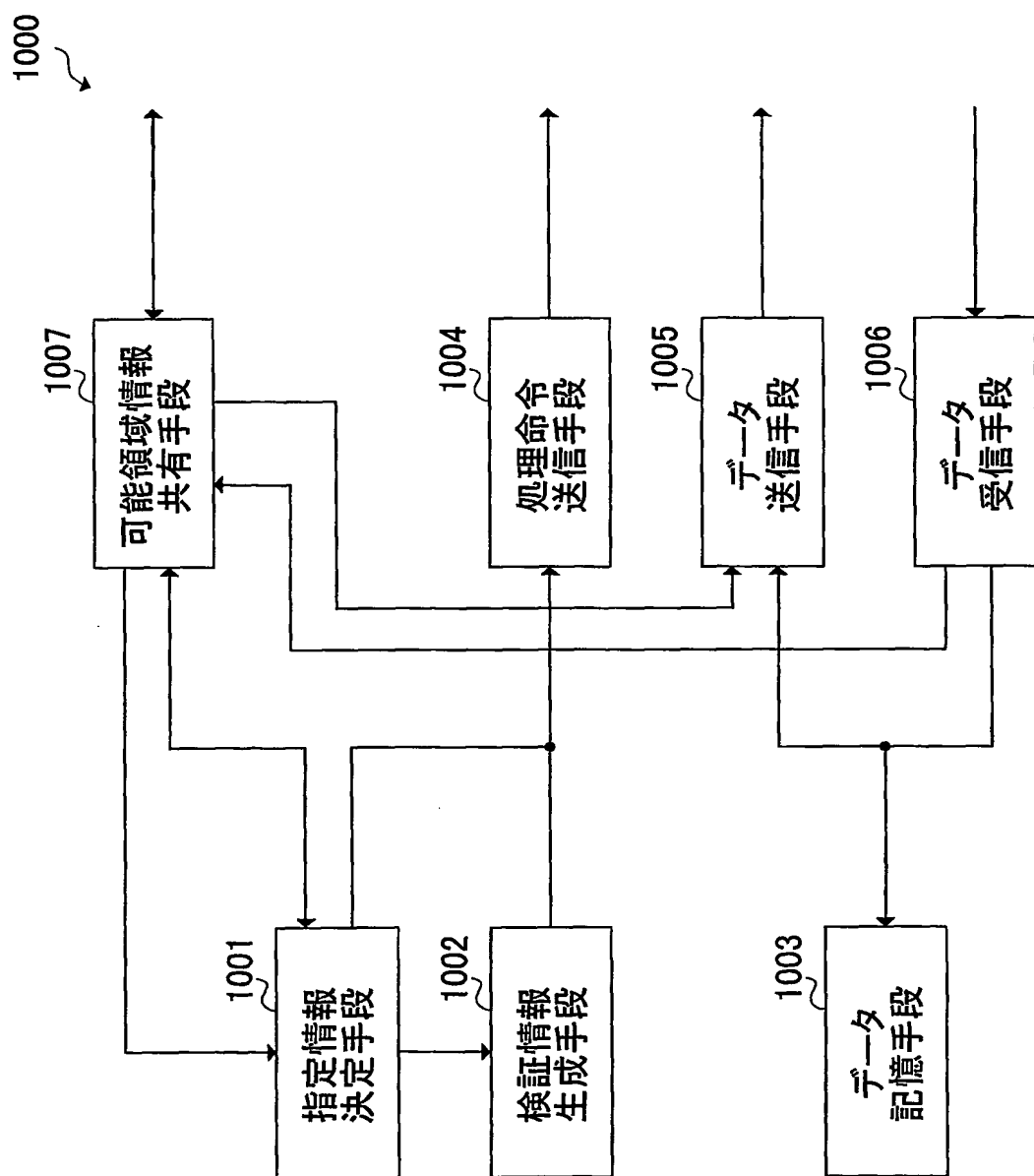


図43

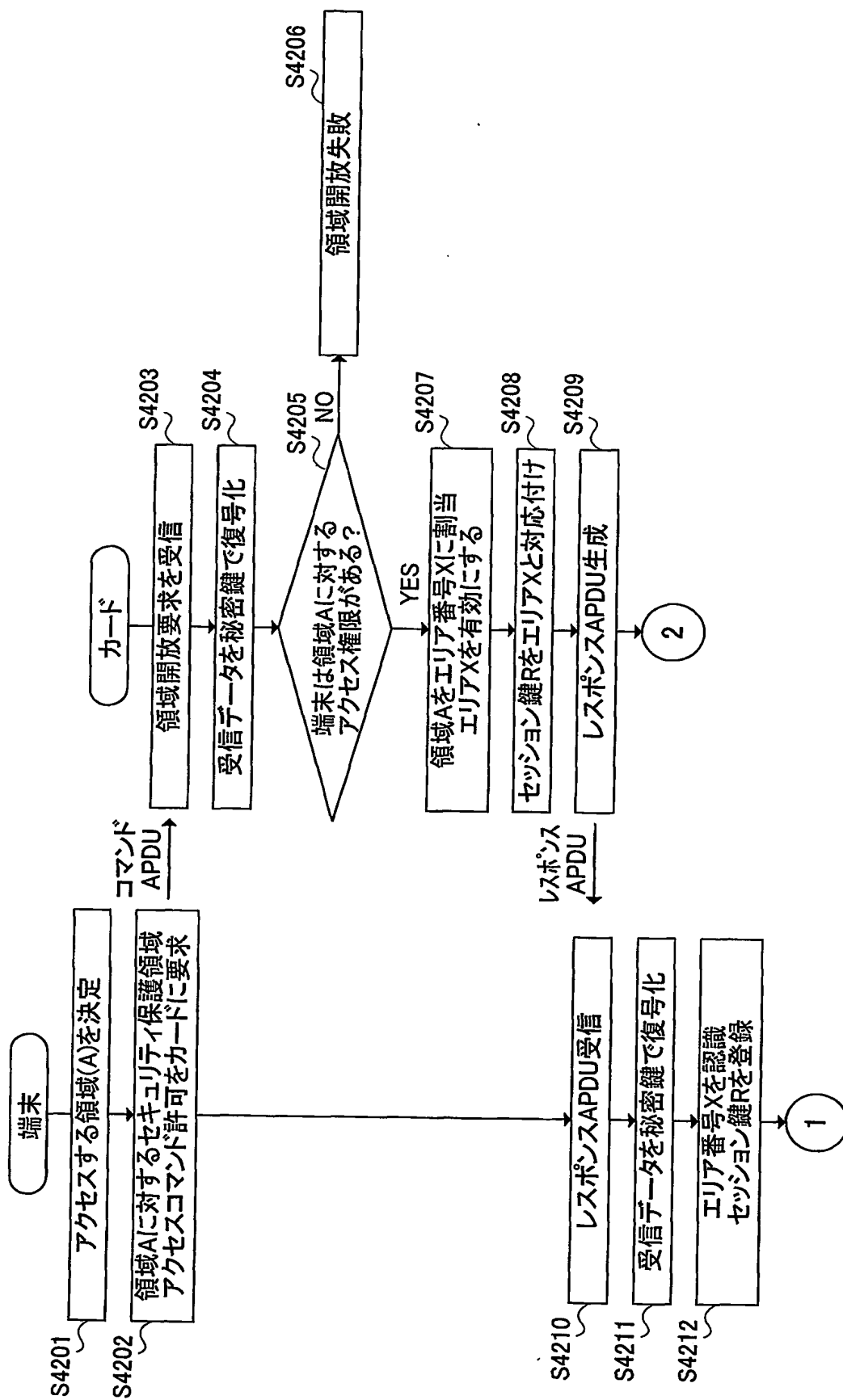


図44

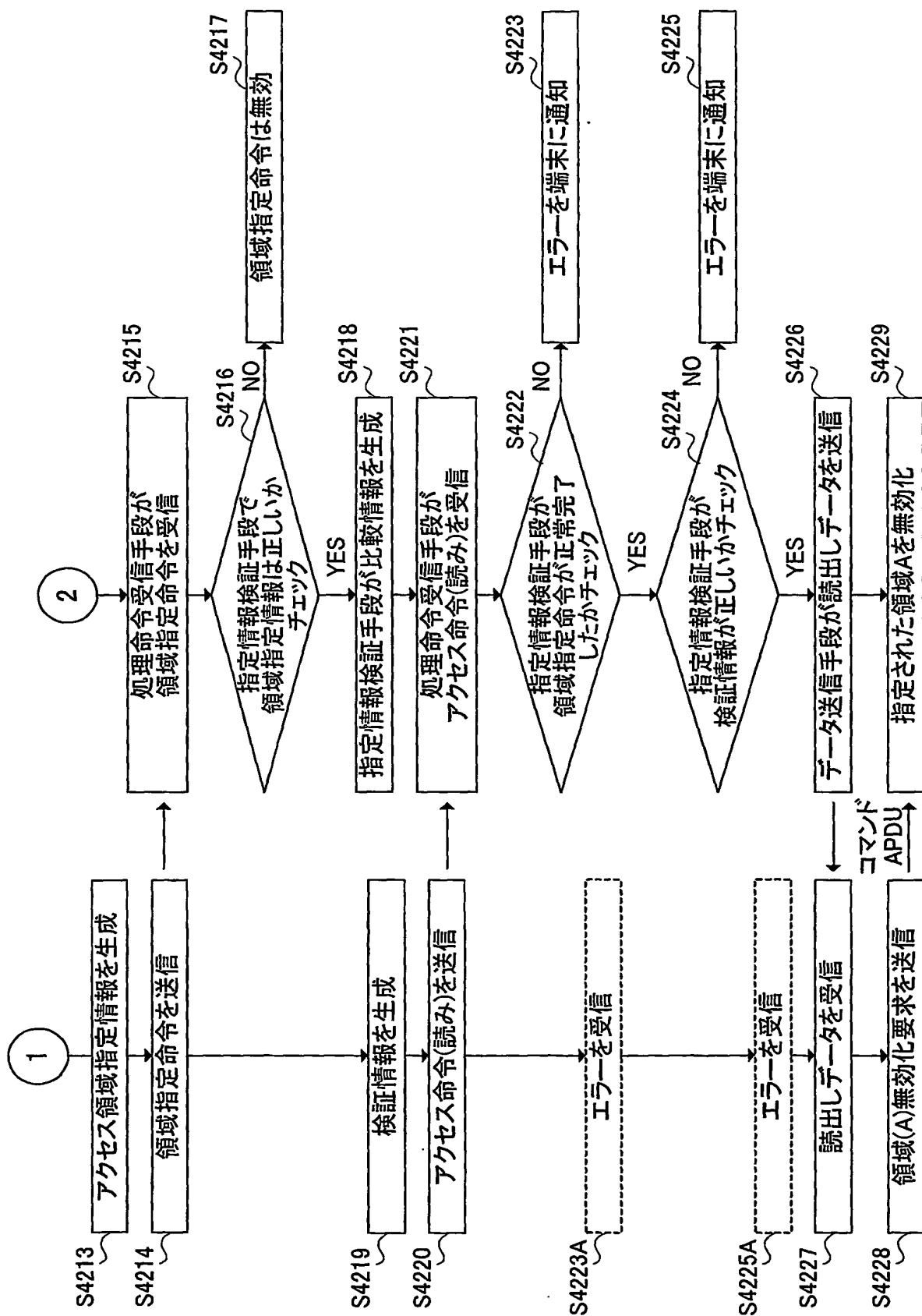


図45

4400
↙

エリア番号X	領域識別子a	検証用鍵R
エリア番号2	領域識別子b	検証用鍵
エリア番号3	領域識別子c	検証用鍵
...

図46

4500
↙

エリア番号X	FILE3	セッション鍵Km
エリア番号2	ファイル識別子2	セッション鍵
エリア番号3	ファイル識別子4	セッション鍵
...

図47

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/010432

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, G06K17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, G06K17/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004

Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-306088 A (Toppan Printing Co., Ltd.), 05 November, 1999 (05.11.99), Full text; all drawings (Family: none)	1-19
Y	JP 1-147686 A (Toshiba Corp.), 09 June, 1989 (09.06.89), Full text; all drawings (Family: none)	1-19
Y	JP 2001-118034 A (Toshiba Corp.), 27 April, 2001 (27.04.01), Full text; all drawings (Family: none)	3-4, 6, 8, 11, 15, 18-19

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
20 October, 2004 (20.10.04)Date of mailing of the international search report
09 November, 2004 (09.11.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/010432

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 7-78126 A (Kyodo Printing Co., Ltd.), 20 March, 1995 (20.03.95), Par. No. [0018]; Fig. 4 (Family: none)	7-8, 19

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl. 7 G06F 12/14, G06K 17/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl. 7 G06F 12/14, G06K 17/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国実用新案登録公報 1996-2004年

日本国登録実用新案公報 1994-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 11-306088 A (凸版印刷株式会社) 1999. 11. 05, 全文, 全図 (ファミリーなし)	1-19
Y	JP 1-147686 A (株式会社東芝) 1989. 06. 09, 全文, 全図 (ファミリーなし)	1-19
Y	JP 2001-118034 A (株式会社東芝) 2001. 04. 27, 全文, 全図 (ファミリーなし)	3-4, 6, 8, 11, 15, 18-19

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

20.10.2004

国際調査報告の発送日

09.11.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

桜井 茂行

5N

2945

電話番号 03-3581-1101 内線 3585

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 7-78126 A (共同印刷株式会社) 1995. 03. 20, 【0018】段落, 第4図 (ファミリーなし)	7-8, 19

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.